IBM Spectrum Protect Knowledge Center Version 8.1.5

Оглавление

Глоссарий 2257

Документация IBM Spectrum Protect

IBM Spectrum Protect предоставляет возможности автоматизации, централизованного планирования и использования политики для управления процессами резервного копирования, архивирования и управления пространством для файл-серверов, рабочих станций, виртуальных машин и прикладных программ. Документация IBM Spectrum Protect помогает установить решения по защите, сконфигурировать их и управлять ими.

Начинаем работу

Установка и обновление серверов
Установка и обновление Центра операций
Выбор и реализация решений по защите данных
Что нового для сервера
Что нового в видеоматериалах
Файлы PDF

Общие задачи

Задачи ежедневного мониторинга
Добавление клиентов
Репликация данных клиента на другой сервер
Управление сервером, клиентами и центром операций
Конфигурирование хранения
Серверные команды, опции и утилиты

Устранение неполадок и поддержка

Диагностика ошибок
Оптимизация производительности
Последние пакеты исправлений для клиентов и серверов IBM Spectrum Protect
Служба поддержки программ IBM

Дополнительная информация

Советы пользователям IBM® Knowledge Center
Комплекты продуктов и связанные продукты
Главная страница семейства продуктов
Википедия для продуктов IBM Spectrum Protect
Центр разработчиков IBM Spectrum Protect
Публикации IBM Redbook
IBM Skills Gateway для компьютеров
Специальные возможности
Юридические замечания для продукта

Специальные возможности для семейства продуктов IBM Spectrum Protect

Специальные возможности помогают пользователю с физическими недостатками, например, с ограниченной подвижностью или с недостатками зрения, с успехом пользоваться продуктами информационных технологий.

Обзор

Продукты семейства IBM Spectrum Protect поддерживают следующие основные специальные возможности:

- Выполнение операций только с помощью клавиатуры (без использования мыши);
- Операции с использованием программы для чтения информации с экрана

Семейство продуктов IBM Spectrum Protect использует новейший стандарт W3C, WAI-ARIA 1.0, чтобы обеспечить соответствие разделу US Section 508 и рекомендациям по доступности веб-содержимого (Web Content Accessibility Guidelines (WCAG) 2.0. Чтобы воспользоваться преимуществами специальных возможностей, возьмите последний выпуск вашей программы чтения информации с экрана и последний веб-браузер, поддерживаемый продуктом.

Документация по продукту в центре знаний IBM включена для поддержки специальных возможностей. Специальные возможности центра знаний IBM описаны в разделе Специальные возможности справки по центру знаний IBM .

Управление при помощи клавиатуры

Для управления этим продуктом используются стандартные комбинации клавиш.

Информация об интерфейсе

В пользовательских интерфейсах нет содержимого, которое бы мигало 2-55 раз в секунду.

В пользовательских веб-интерфейсах правильное воспроизведение содержимого и подходящий для работы режим основаны на каскадных таблицах стилей. Приложение обеспечивает пользователям со слабым зрением эквивалентный способ использовать параметры системного дисплея, включая высококонтрастный режим. Можно управлять размером шрифта, используя параметры устройства или веб-браузера.

В пользовательских веб-интерфейсах есть навигационные отметки WAI-ARIA, которые позволяют быстро переходить к функциональным областям в приложении.

Программное обеспечение поставщиков

В семейство продуктов IBM Spectrum Protect включены программы некоторых поставщиков, на которые не распространяется лицензионное соглашение IBM. IBM не делает никаких заявлений относительно специальных возможностей этих продуктов. За информацией о специальных возможностях этих продуктов обращайтесь к их поставщикам.

Прочие сведения о специальных возможностях

Помимо стандартной консультативно-справочной службы IBM и веб-сайтов поддержки у IBM есть две телефонные службы TTY для использования глухими или слабо слышащими заказчиками с целью получения доступа к службам продаж и поддержки:

Служба TTY
800-IBM-3383 (800-426-3383)
(в Северной Америке)

Дополнительную информацию об обязательствах, которые IBM принимает на себя в отношении поддержки специальных возможностей, смотрите на сайте IBM Accessibility.

Комплекты продуктов и связанные продукты

IBM Spectrum Storage Suite и связанные продукты хранения совершенствуют и расширяют возможности базового продукта IBM Spectrum Protect.

Комплекты продуктов и опции лицензий

Продукты IBM Spectrum Protect и IBM Spectrum Protect Extended Edition предлагают основные компоненты для автоматизированных и централизованных операций резервного копирования и восстановления. Компоненты сервера и клиента резервного копирования и архивирования обеспечивают такие основные функции, как операции резервного копирования и восстановления, а также операции архивирования и получения для файлов, каталогов и образов дисков.

Документация по продукту содержит информацию как по IBM Spectrum Protect, так и по IBM Spectrum Protect Extended Edition.

Комплекты продуктов, в которых IBM Spectrum Protect комбинируется со связанными продуктами, могут оказаться более удобным способом покупки программы и управления ею. Комплекты содержат продукты, способные выполнить широкий спектр требований к защите данных и восстановлению при упрощенном лицензировании.

Выберите комплект продуктов, соответствующий вашим бизнес-требованиям:

- Информацию о комплектах продуктов IBM Spectrum Protect смотрите в техническом замечании 7048916.
- Информацию о IBM Spectrum Storage Suite, содержащем IBM Spectrum Protect и другие продукты, смотрите в документе IBM Spectrum Storage Suite.

Связанные продукты

IBM Spectrum Protect можно расширить за счет функций и компонентов, имеющихся в связанных продуктах.

Продукт	**Важнейшие преимущества**	**Связи**
IBM® Cloud Object Storage	Обеспечивает веб-платформу для хранения неструктурированных данных от петабайтов до экзабайтов.	• Узнать подробнее и купить
IBM Spectrum Control	Обеспечивает управление аналитическими данными.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Copy Data Management	Каталогизирует снимки NetApp и VMware для упрощения управления на основе ролей и восстановления резервных копий данных.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect High Speed Data Transfer	Этот продукт используется для включения поддержки технологии Fast Adaptive Secure Protocol (FASP), улучшающей передачу данных в среде региональной сети (wide area network, WAN), где выявляются проблемы с производительностью.	• Узнать подробнее и купить • Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде
IBM Spectrum Protect for Data Retention	Обеспечивает защиту долгосрочного хранения при архивировании бизнес-записей, файлов или данных. Архивирование данных в соответствии с нормативными требованиями требует больше предосторожностей или более сильную защиту, которая называется защитой хранения данных. Эти меры предосторожности помогут убедиться, что данные не будут стерты преждевременно ни случайно, ни по злому умыслу. Чтобы выполнить требования пор соответствию, IBM Spectrum Protect for Data Retention обеспечивает больше защиты для данных, чем это достигается при использовании IBM Spectrum Protect.	• Узнать подробнее и купить • Документация по продукту Совет: Документация по этому продукту включена в документацию по IBM Spectrum Protect.
IBM Spectrum Protect Plus	Предоставляет решение защиты данных и доступности для виртуальных сред, которое можно внедрить за несколько минут и которое защитит среду в течение часа. IBM Spectrum Protect Plus можно реализовать как автономное решение или интегрировать решение со средой IBM Spectrum Protect для выгрузки копий для долгосрочного хранения и управления масштабируемостью и эффективностью.	

Продукт	Важнейшие преимущества	Связи
IBM Spectrum Protect Snapshot	Защищает данные благодаря встроенным возможностям резервного копирования и восстановления снимков с учетом состояния прикладной программы. Данные, хранимые прикладными программами IBM DB2, SAP, Oracle, Microsoft Exchange и Microsoft SQL Server, можно защитить с помощью программного обеспечения IBM Spectrum Protect Snapshot. При помощи программы можно создавать снимки на уровне томов для файловых систем и пользовательских приложений и управлять ими. Можно выбрать, интегрировать ли IBM Spectrum Protect Snapshot с IBM Spectrum Protect.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect for Databases	Защищает данные Oracle и данные Microsoft SQL посредством применения автоматизированных задач, утилит и интерфейсов. Эта программа создает онлайновые, непротиворечивые и централизованные резервные копии, которые помогут вам избежать отключений, защитить жизненно важные данные предприятия и свести к минимуму рабочие затраты. Совет: Поддержка онлайновых резервных копий баз данных IBM DB2 и IBM Informix включена в серверы IBM Spectrum Protect. Устанавливать IBM Spectrum Protect for Databases для резервного копирования этих баз данных не нужно. Дополнительную информацию смотрите в документации по продуктам DB2 и Informix.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect for Enterprise Resource Planning	Предоставляет защиту, настраиваемую для данных системы SAP.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect for Mail	Автоматизированная защита данных, при которой операции резервного копирования выполняются без остановки серверов Microsoft Exchange и серверов IBM Domino.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect for Space Management	Продукт по управлению иерархическим пространством хранения, который сокращает затраты на информацию, доступ к которой осуществляется редко, не изменяя способ взаимодействия пользователей и приложений с данными. Используйте этот продукт в операционных системах IBM AIX и Linux.	• Узнать подробнее и купить • Документация по продукту

Продукт	Важнейшие преимущества	Связи
IBM Spectrum Protect HSM for Windows	Продукт по управлению иерархическим пространством хранения, который сокращает затраты на информацию, доступ к которой осуществляется редко, не изменяя способ взаимодействия пользователей и приложений с данными. Используйте этот продукт в операционных системах Microsoft Windows.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Protect for SAN	Работает с серверами и компьютерами клиентов для передачи данных через сеть хранения данных (SAN), используемую вместо локальной сети (local area network, LAN). Продукт представляет собой агент хранения, позволяющий производить операции резервного копирования и восстановления без использования локальной сети.	• Узнать подробнее и купить • Документация по продукту Версия документации к продукту: Документацию к IBM Tivoli Storage Manager for SAN версии 7.1 можно использовать с семейством продуктов IBM Spectrum Protect версии 8.1.
IBM Spectrum Protect for Virtual Environments	Предоставляет защиту, настраиваемую для виртуальных сред VMware и Hyper-V.	• Узнать подробнее и купить • Документация по продукту
IBM Spectrum Scale	Обеспечивает масштабируемое хранение неструктурированных данных.	• Узнать подробнее и купить • Документация по продукту
IBM Tivoli Storage Manager for z/OS Media	Управляет дисковыми и ленточными ресурсами z/OS для серверов IBM Spectrum Protect, работающих в системах AIX или Linux on System z.	• Документация по продукту

Файлы PDF

Предварительно встроенные файлы PDF можно скачать из центра знаний IBM® или с сайта скачивания FTP.

Предварительно построенные файлы PDF

Чтобы узнать о том, какие предварительно встроенные файлы PDF доступны для этого выпуска, смотрите следующие разделы:

- Решения для защиты данных
- Серверы

Пакет для файлов PDF

Скачайте пакет, содержащий все файлы PDF для данного выпуска, со следующего FTP-сайта:

ftp://public.dhe.ibm.com/software/products/ISP/current/

Обновления в этом выпуске

Прочтите о новых функциях и усовершенствованиях, которые есть в продуктах, чтобы узнать о потенциальных преимуществах для ваших операций по управлению хранением. Замечания по выпуску содержат ссылки, используя которые, вы сможете получить важную информацию, прежде чем будете устанавливать или обновлять продукты и компоненты.

Компонент	Сводка обновлений	Замечания по выпуску V8.1

Компонент	Сводка обновлений	Замечания по выпуску V8.1
Серверные компоненты	Обновления	Замечания по выпуску

- Бета-программа
  Бета-программа IBM Spectrum Protect позволяет впервые взглянуть на появившиеся функции продукта и дает возможность повлиять на изменения при его проектировании. Вы сможете протестировать новую программу в своей системной среде и непосредственно высказать свое мнение в процессе разработки продукта.

Понятия, связанные с IBM Spectrum Protect

IBM Spectrum Protect обеспечивает всеобъемлющую среду защиты данных.

- IBM Spectrum Protect - Обзор
  IBM Spectrum Protect обеспечивает централизованную, автоматизированную защиту данных, помогающую уменьшить потерю данных и управлять соответствием с требованиями к хранению данных и их доступности.
- Понятия, касающиеся хранения данных в IBM Spectrum Protect
  В IBM Spectrum Protect есть функции для хранения данных на различных устройствах и носителях.
- Стратегии защиты данных с использованием IBM Spectrum Protect
  IBM Spectrum Protect обеспечивает возможность реализовать различные стратегии защиты данных.

IBM Spectrum Protect - Обзор

IBM Spectrum Protect обеспечивает централизованную, автоматизированную защиту данных, помогающую уменьшить потерю данных и управлять соответствием с требованиями к хранению данных и их доступности.

- Компоненты защиты данных
  Решения по защите данных, которые обеспечивает IBM Spectrum Protect, состоят из сервера, клиентских систем и приложений и носителей хранения. IBM Spectrum Protect обеспечивает интерфейсы управления для мониторинга и создания отчетов о состоянии защиты данных.
- Службы защиты данных
  IBM Spectrum Protect обеспечивает службы защиты данных для хранения и восстановления данных с различных типов клиентов. Службы защиты данных реализованы через политики, заданные на сервере. Чтобы автоматизировать службы защиты данных, можно использовать планирование клиента.
- Процессы для управления защитой данных в IBM Spectrum Protect
  Перечень серверов IBM Spectrum Protect выполняет важнейшую роль в процессах защиты данных. Вы задаете политики, которые сервер использует для управления хранением данных.
- Пользовательские интерфейсы для среды IBM Spectrum Protect.
  Для выполнения задач по мониторингу и конфигурированию в IBM Spectrum Protect есть различные интерфейсы, включая центр операций, интерфейс командной строки и административный интерфейс SQL.

Компоненты защиты данных

Решения по защите данных, которые обеспечивает IBM Spectrum Protect, состоят из сервера, клиентских систем и приложений и носителей хранения. IBM Spectrum Protect обеспечивает интерфейсы управления для мониторинга и создания отчетов о состоянии защиты данных.

Сервер

Системы клиентов отправляют данные на сервер, чтобы они были сохранены как резервные копии или архивные данные. На сервере есть *перечень*, представляющий собой репозиторий информации о данных клиента.

Перечень содержит следующие компоненты:

Database
: В базе данных сервера хранятся созданные сервером резервные копии, архивы или перенесенные данные для каждого файла, логического тома или базы данных. База данных сервера также содержит информацию о политике и расписаниях для служб защиты данных.

Журнал восстановления

В этом журнале хранятся записи о транзакциях базы данных. База данных использует журнал восстановления, чтобы обеспечить непротиворечивость данных в базе данных.

Системы и приложения клиентов

Клиенты - это приложения, виртуальные машины и системы, которые нужно защитить. Клиенты отправляют данные на сервер, как показано на Рис. 1.

Рис. 1. Компоненты в решении по защите данных

Программа клиента
: Чтобы IBM Spectrum Protect защищал данные клиента, в системах клиентов должна быть установлена соответствующая программа, и клиент должен быть зарегистрирован на сервере.

Клиентские узлы
: *Клиентский узел* эквивалентен компьютеру, виртуальной машине или приложению, например, клиенту резервного копирования и архивирования, который устанавливается на рабочей станции для резервного копирования файловой системы. Каждый клиентский узел должен быть зарегистрирован на сервере. На одном компьютере можно зарегистрировать несколько узлов.

Носитель хранения

Сервер сохраняет данные клиента на носителе хранения. Используются следующие типы носителей:

Устройства хранения
: Сервер может записывать данные на жесткие диски, в массивы дисков, в подсистемы дисков, на автономные ленточные накопители, в ленточные библиотеки и на другие виды носителей хранения с произвольным и последовательным доступом. Устройства хранения могут быть непосредственно подключены к серверу или могут быть подключены через локальную сеть или сеть хранения данных (SAN).

Пулы хранения
: Устройства хранения, соединенные с сервером, группируются в *пулы хранения*. Каждый пул хранения представляет собой набор устройств хранения с одним и тем же типом носителей (например, дисковых или ленточных накопителей). IBM Spectrum Protect хранит все даные клиенртов в пулах хранения. Пулы хранения можно организовать в *иерархию*, так чтобы хранящиеся данные можно было переносить из дискового пространства хранения в более экономичное пространство хранение, например, на ленточные устройства.

Службы защиты данных

IBM Spectrum Protect обеспечивает службы защиты данных для хранения и восстановления данных с различных типов клиентов. Службы защиты данных реализованы через политики, заданные на сервере. Чтобы автоматизировать службы защиты данных, можно использовать планирование клиента.

Типы служб защиты данных

В IBM Spectrum Protect есть службы для сохранения и восстановления данных клиента, как показано на Рис. 1.

Рис. 1. Службы защиты данных

В IBM Spectrum Protect есть следующие типы служб защиты данных:

Службы резервного копирования и восстановления

ВЫ запускаете процесс резервного копирования для создания копии *объекта данных*, которую можно будет использовать для восстановления, если исходный объект данных будет потерян. Объектом данных могут быть файл, каталог или заданный пользователем объект данных, например, база данных.

Чтобы свести к минимуму использование системных ресурсов во время операции резервного копирования, IBM Spectrum Protect использует метод *прогрессивного инкрементного резервного копирования*. При таком методе резервного копирования создается первая полная резервная копия всех объектов данных, а при последующих операциях резервного копирования в хранилище перемещаются только изменившиеся данные. По сравнению с методом инкрементного и дифференциальное резервного копирования, при использовании которых периодически требуются создавать полные резервные копии, прогрессивный метод инкрементного резервного копирования обеспечивает следующие преимущества:

- Снижает степень дублирования данных
- Использует меньшую полосу пропускания
- Требует меньше пространства в пуле хранения

Чтобы дополнительно снизить требования к емкости хранения и использованию сетевой полосы пропускания, IBM Spectrum Protect использует *дедупликацию данных* при резервном копировании данных. Метод дедупликации данных позволяет удалить дубликаты экстентов данных из резервных копий.

Чтобы скопировать объект из пула хранения на клиент, вы используете процесс восстановления. Можно восстановить один файл, все файлы в каталоге или все данные на компьютере.

Службы архивирования и получения

Вы используете службу архивирования для сохранения данных, которые нужно хранить в течение длительного времени (например, в соответствии с нормативами). Служба архивирования обеспечивает следующие возможности:

- При архивировании данных вы указываете, сколько времени должны храниться данные.
- Можно указать, что файлы и каталоги копируются на носитель для долгосрочного хранения. Например, вы можете выбрать хранение таких данных на ленточном устройстве, что позволит сократить затраты на хранение.
- Можно также указать, что после архивирования исходные файлы стираются с клиента.

Служба получения обеспечивает следующие возможности:

- Когда вы получаете даные, они копируются из пула хранения на клиентский узел.
- При получении данных архивная копия остается в пуле хранения.

Службы переноса и возврата

Для управления пространством в системах клиентов используются службы переноса и возврата. Цель управления пространством - максимизировать доступную емкость носителя и минимизировать время доступа к данным. Вы можете перенести данные в серверное хранилище, чтобы обеспечить достаточный объем свободного пространства в локальной файловой системе. Перенесенные данные можно сохранить следующими способами:

- В дисковом пространстве хранения в случае долгосрочного хранения
- В *виртуальной ленточной библиотеке* (Virtual Tape Library, VTL) для быстрого возврата файлов

Вы можете возвращать файлы на клиентский узел по требованию (автоматически или выборочно).

Типы данных клиента, которые можно защитить

Данные можно защитить для следующих типов клиентов с IBM Spectrum Protect:

Клиенты приложения
: IBM Spectrum Protect позволяет защитить данные для отдельных продуктов или приложений. Эти клиенты называются *клиентами приложений*. Чтобы защитить для этих клиентов *структурированные данные*, другими словами, данные в полях базы данных, нужно создать резервные копии компонентов, связанных с приложением. IBM Spectrum Protect может защитить следующие приложения:

  - Клиенты IBM Spectrum Protect for Enterprise Resource Planning:
    - Data Protection for SAP HANA
    - Data Protection for SAP for DB2
    - Data Protection for SAP for Oracle
  - Клиенты IBM Spectrum Protect for Databases:
    - Data Protection for Microsoft SQL Server
    - Data Protection for Oracle
  - Клиенты IBM Spectrum Protect for Mail:
    - Data Protection for IBM® Domino
    - Data Protection for Microsoft Exchange Server

Виртуальные машины
: Виртуальные машины, резервное копирование которых производится с использованием программы приложения-клиента, установленного на виртуальной машине. В среде IBM Spectrum Protect защиту виртуальной машины может обеспечить IBM Spectrum Protect for Virtual Environments.

Клиенты компьютера
: Перечисленные ниже клиенты IBM Spectrum Protect называются *системными клиентами*:

  - Все клиенты, которые создают резервные копии данных в файлах и каталогах, другими словами *неструктурированных данных*, например, клиенты резервного копирования и архивирования и клиенты API, установленные на рабочих станциях.
  - Сервер, включенный в конфигурацию виртуального тома сервер-сервер.
  - Виртуальная машина, резервная копия которой создается с использованием программы клиента резервного копирования и архивирования, установленной на виртуальной машине.

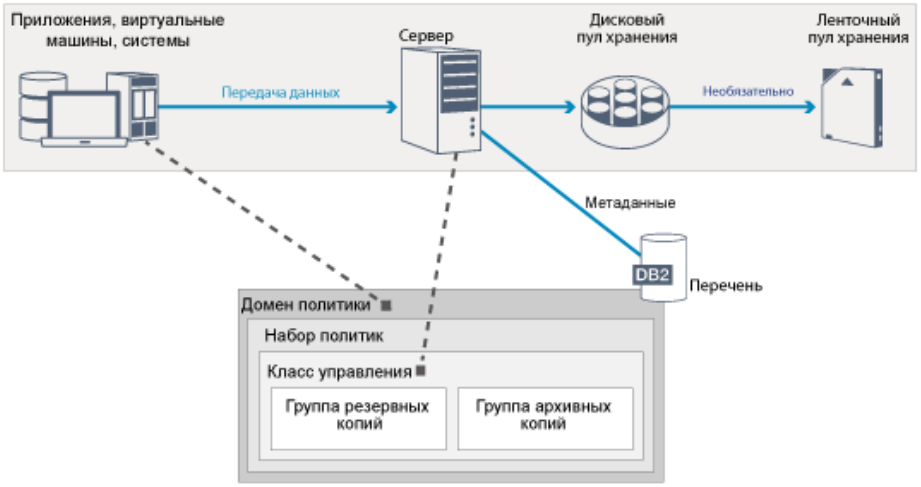
Процессы для управления защитой данных в IBM Spectrum Protect

Перечень серверов IBM Spectrum Protect выполняет важнейшую роль в процессах защиты данных. Вы задаете политики, которые сервер использует для управления хранением данных.

Процесс управления данными

На Рис. 1 показан процесс управления данными IBM Spectrum Protect.

Рис. 1. Процесс управления данными



IBM Spectrum Protect использует политики для управления тем, как сервер сохраняет объекты данных и управляет ими на устройствах хранения и носителях различных типов. Вы связываете клиент с доменом политики, содержащим один активный набор политик. Когда клиент выполняет резервное копирование, архивирование или перенос файла, файл привязывается к классу управления в активном наборе политик домена политики. Класс управления и содержащиеся в нем группы резервного копирования и архивирования задают, где хранятся файлы и как они управляются. Если вы настроили хранение сервера в иерархии, вы можете переносить файлы в разные пулы хранения.

Компоненты перечня

Перечисленные ниже компоненты перечня являются ключом к работе сервера:

База данных сервера
: База данных серверасодержит информацию о данных клиента и операциях сервера. В базе данных хранится информация о данных клиента, которые называются *метаданными*. Сведения о данных клиента включают в себя имя файла, размер файла, имя владельца файла, класс управления, группу копирования и положение файла в хранении сервера. База данных содержит следующую информацию, необходимую для работы сервера:

  - Определения клиентских узлов и администраторов
  - Правила политики и расписания
  - Параметры сервера
  - Записи об операциях сервера, например, журналы операций и записи о событиях
  - Промежуточные результаты административных запросов

Журнал восстановления
: Сервер записывает транзакции базы данных в журнал восстановления. Журнал восстановления нужен для того, чтобы в случае сбоя база данных не осталась в несогласованном состоянии. Журнал восстановления также используется, чтобы обеспечить непротиворечивость данных для разных операций по запуску сервера. Журнал восстановления состоит из следующих журналов:

  Активный журнал
  : В этот журнал записываются текущие транзакции на сервере. Эта информация необходима для того, чтобы можно было запустить сервер и базу данных после аварии.

  Зеркальная копия журнала (необязательно)
  : Зеркальная копия активного журнала - это копия активного журнала, которую можно использовать, если не удастся прочитать файлы активного журнала. Все изменения, записываемые в активный журнал, также записываются в зеркальную копию журнала. Вы можете задать только одну зеркальную копию активного журнала.

  Архивный журнал
  : В архивном журнале содержатся копии закрытых файлов журнала, которые находились в активном журнале. Архивный журнал включен в резервное копирование базы данных и используется для восстановления базы данных сервера. Файлы архивного журнала, включенные в резервное копирование базы данных, автоматически отбрасываются по завершении цикла полного резервного копирования базы данных. В архивном журнале должно быть достаточно места для сохранения файлов журнала для операций резервного копирования базы данных.

  Резервный архивный журнал (необязательно)

Резервный архивный журнал, который также называют вторичным архивным журналом - это каталог, который используется сервером для сохранения файлов архивного журнала в случае переполнения каталога архивного журнала.

Управление данными на основе политик

В среде IBM Spectrum Protect *политика* по защите данных содержит правила, которые определяют способы хранения данных и управления ими. Основной целью политики является реализация следующий целей по управлению данными:

- Управление тем, в каком пуле хранения первоначально сохраняются данные клиента
- Назначение критериев хранения, которые управляют тем, сколько копий объектов хранится
- Назначение сроков хранения копий объектов

Управление данными на основе политик дает возможность уделить основное внимание бизнес-требованиям по защите данных, а не управлению устройствами и носителями хранения. Администраторы задают политики и назначают клиентские узлы в *домен политики*.

В зависимости от бизнес-потребностей можно задать одну политику или несколько. В бизнес-организации, например, у разных отделов с различными типами данных могут быть настроенные планы управления хранением. Политики можно изменить, и изменения можно применить к уже управляемым данным.

При установке IBM Spectrum Protect уже задана политика по умолчанию STANDARD. Политика STANDARD обеспечивает базовый уровень защиты резервного копирования для рабочих станций пользователей. Политику по умолчанию можно изменить или создать новую, чтобы предоставлять клиентам разные уровни обслуживания.

Вы создаете политики, задавая следующие компоненты политики:

Домен политики
: Домен политики - это основной организационный метод группирования клиентских узлов, которые совместно используют общие правила для управления данными. Хотя клиентский узел можно задать для нескольких серверов, его можно задать только для одного домена политики на каждом сервере.

Набор политик
: *Набор политик* - это ряд политик, сгруппированных так, чтобы политику для клиентских узлов в домене можно было активировать или деактивировать нужным образом. Администратор использует набор политик для реализации разных классов управления в зависимости от бизнес-требований и требований пользователей. Домен политики может содержать несколько наборов политик, но в домене может быть активен только один набор. Каждый набор политик содержит класс управления по умолчанию и любое число дополнительных классов управления.

Класс управления
: *Класс управления* - это объект политики, который можно связать с каждой категорией данных, чтобы указать, как сервер управляет данными. Может существовать один или несколько классов управления. Один класс управления назначается как класс управления по умолчанию, который используется клиентами, если для них явным образом не переопределен класс по умолчанию, так чтобы они использовали специальный класс управления.

  В классе управления может содержаться группа резервных копий, группа архивных копий и атрибуты управления пространством. Группа копий определяет, как сервер управляет резервными версиями или архивными копиями файла. Атрибуты управления пространством определяют, подлежит ли файл переносу клиентом менеджера по пространству в серверное хранилище и при каких условиях производится перенос файла.

Группа копирования
: *Группа копий* - это набор атрибутов в классе управления, который управляет следующими факторами:

  - Где сервер хранит версии резервных копий файлов или архивных копий
  - Как долго сервер хранит версии резервных копий файлов или архивных копий
  - Сколько версий резервных копий следует хранить
  - Какой метод следует использовать для генерирования версий резервных копий файлов или архивных копий

Управление защитой

IBM Spectrum Protect содержит ряд функций для регистрации администраторов и пользователей. После регистрации администраторов им нужно предоставить полномочия, назначив для них один или несколько классов административных полномочий. Администратор с системными полномочиями может выполнять на сервере любые функции. Администраторы, обладающие полномочиями на управление политиками, хранилищем, операторами или узлами, могут

выполнять только определенное подмножество функций сервера. Доступ к серверу можно получить следующими способами, каждый из которых управляется паролем:

- Доступ администратора для управления сервером
- Доступ клиента к узлам для сохранения и получения данных

Также включены функции, которые могут помочь обеспечить защиту, когда клиенты соединяются с сервером. Если вы являетесь администратором, то, в зависимости от бизнес-требований, вы можете выбрать один из следующих методов регистрации клиентов:

Открытая регистрация
: Когда клиент впервые соединяется с сервером, у пользователя запрашивают имя узла, пароль и контактную информацию. Открытая регистрация обеспечивает пользователю следующие параметры по умолчанию:

  - Клиентский узел назначается в домен политики STANDARD.
  - Пользователь может указать, следует ли производить сжатие файлов с целью уменьшения объема данных, пересылаемых по сети, а также какое пространство будет занято данными в хранилище.
  - Пользователь может удалить из серверного хранилища архивные копии файлов, но не версии резервных копий файлов.

Закрытая регистрация
: Закрытая регистрация - это способ регистрации клиентов по умолчанию на сервере. При таком типе регистрации администратор регистрирует всех клиентов. Администратор может реализовать следующие параметры:

  - Назначить узел в любой домен политики
  - Указать, может ли пользователь использовать сжатие, или нет, либо может дать пользователя возможность выбрать
  - Управлять тем, может ли пользователь удалять резервные копии файлов или архивные файлы

Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL). SSL - это стандартная технология, которую вы используете для создания зашифрованных сеансов для серверов и клиентов и которая обеспечивает безопасный канал связи для взаимодействий по открытым путям связи. При использовании SSL идентификационная информация сервера проверяется с помощью цифровых сертификатов. Если вы производите аутентификацию на основе паролей на сервере Lightweight Directory Access Protocol (LDAP), пароли между сервером и сервером LDAP будут защищены протоколом Transport Layer Security (TLS). Протокол TLS - это преемник протокола SSL. Когда сервер и клиент взаимодействуют, TLS гарантирует, что третья сторона не сможет перехватывать сообщения.

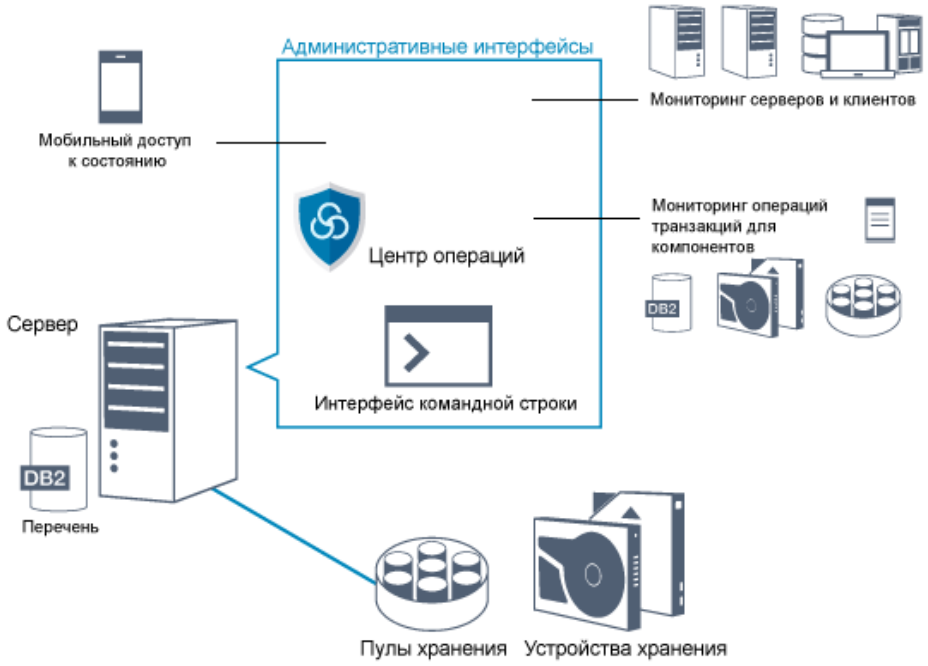
Пользовательские интерфейсы для среды IBM Spectrum Protect.

Для выполнения задач по мониторингу и конфигурированию в IBM Spectrum Protect есть различные интерфейсы, включая центр операций, интерфейс командной строки и административный интерфейс SQL.

Интерфейсы для управления хранением данных

Центр операций - это основной интерфейс для администраторов, позволяющий производить мониторинг и администрирование серверов. Важнейшее преимущество центра операций в том, что можно производить мониторинг нескольких серверов, как показано на Рис. 1. Также можно производить мониторинг и администрирование IBM Spectrum Protect из административного интерфейса командной строки.

Рис. 1. Интерфейсы пользователяя для управления хранением данных



Для взаимодействия с IBM Spectrum Protect можно использовать следующие интерфейсы:

Центр операций
: Центр операций обеспечивает веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Центр операций можно использовать для выполнения задач по мониторингу и некоторых задач по администрированию, например:

  - Можно производить мониторинг нескольких серверов и клиентов.
  - Можно отслеживать активность транзакций для отдельных компонентов в пути данных, например, для базы данных сервера, журнала восстановления, устройств хранения и пулов хранения.

Интерфейс командной строки
: Интерфейс командной строки можно использовать для выполнения задач по администрированию для серверов. Доступ к интерфейсу командной строки можно получить доступ либо через административный клиент IBM Spectrum Protect, либо через центр операций.

Доступ к информации в базе данных сервера с использованием операторов SQL
: Операторы SQL SELECT можно использовать, чтобы запрашивать базу данных сервера и просматривать результаты. Существуют инструменты SQL сторонних поставщиков, помогающие администраторам управлять базами данных.

Интерфейсы для управления операциями клиентов

IBM Spectrum Protect обеспечивает следующие типы интерфейсов для управления операциями клиентов:

- Интерфейс прикладного программирования (API)
- Графические пользовательские интерфейсы для клиентов
- Интерфейс браузера для клиента резервного копирования и архивирования
- Интерфейсы командной строки для клиентов

Понятия, касающиеся хранения данных в IBM Spectrum Protect

В IBM Spectrum Protect есть функции для хранения данных на различных устройствах и носителях.

Чтобы сделать устройства хранения доступными для сервера, нужно подключить устройства хранения и отобразить пулы хранения в классы устройств, библиотеки и накопители.

- Типы устройств хранения
  В сочетании с IBM Spectrum Protect можно использовать различные устройства хранения, чтобы выполнить определенные цели по защите данных.
- Хранение данных в пулах хранения
  Основными компонентами в модели хранения данных IBM Spectrum Protect являются логические пулы хранения.

Использование устройств хранения можно оптимизировать путем управления свойствами пулов хранения и томов.

- Транспорт данных в пространство хранения в разных сетях
  Среда IBM Spectrum Protect обеспечивает возможности безопасного перемещения данных в пространство хранения по разным типам сетей и при разных конфигурациях.

Типы устройств хранения

В сочетании с IBM Spectrum Protect можно использовать различные устройства хранения, чтобы выполнить определенные цели по защите данных.

Устройства хранения и объекты хранения

Сервер IBM Spectrum Protect может соединяться с комбинацией устройств ручного и автоматизированного хранения. К IBM Spectrum Protect можно подключить следующие типы устройств хранения:

- Дисковые устройства с непосредственным подключением, подключением SAN или подключением через сеть.
- Физические ленточные устройства, управляемые вручную или автоматически
- Виртуальные ленточные устройства
- Облачное пространство хранения объектов

IBM Spectrum Protect представляет физические устройства хранения и носители с объектами хранения, которые заданы в базе данных сервера. Объекты хранения классифицируют доступные ресурсы хранения и управляют переносом данных из одного пула хранения в другой. Табл. 1 описывает объекты хранения в среде хранения сервера.

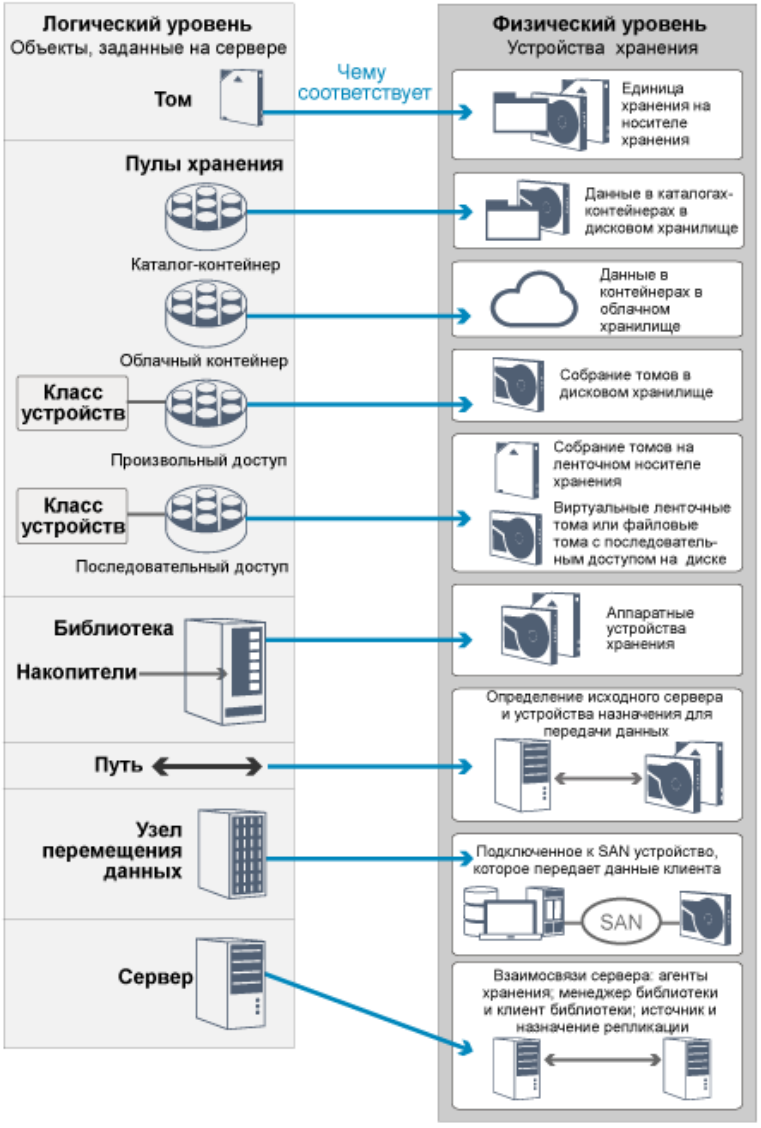
Табл. 1. Объекты хранения, и что они представляют

Объект хранения	**Что представляет объект**
Том	Дискретный блок хранения на диске, ленте или на другом носителе хранения. Каждый том связан с одним пулом хранения.
Пул хранения	Набор томов или контейнеров хранения, которые служат пунктом назначения для хранения данных клиентов. IBM Spectrum Protect использует следующие типы пулов хранения: • Пулы хранения контейнеров каталогов • Пулы хранения облачных контейнеров • Пулы хранения с последовательным доступом, связанные с классом устройств • Пулы хранения с произвольным доступом, связанные с классом устройств
Контейнер	Место хранения данных, например, файл, каталог или устройство.
Пул хранения контейнера	Первичный пул хранения, используемый сервером для хранения данных. Данные хранятся в контейнерах в каталогах файловой системы или в облачном хранилище. Если потребуется, производится дедупликация данных, когда сервер записывает данные в пул хранения.
Класс устройств	Тип устройства хранения, которое может использовать тома, заданные для пула хранения с последовательным или произвольным доступом. Каждый класс устройств типа Съемный носитель связан с одной библиотекой.
Библиотека	Устройство хранения. Например, библиотека может представлять автономный накопитель, набор автономных накопителей, автоматизированное устройство с несколькими накопителями или набор накопителей, которые управляются менеджером носителей.

Объект хранения	Что представляет объект
Накопитель	Объект устройства ленточной библиотеки, обеспечивающий возможность читать и записывать данные на ленточный носитель библиотеки. Каждый накопитель связан с одной библиотекой.
Путь	Спецификация источника данных и назначения устройства. Прежде чем можно будет использовать устройство хранения, должен быть задан путь между устройством и исходным сервером, выполняющим перемещение данных.
Узел перемещения данных	Подключенное к SAN устройство, которое используется для передачи данных клиента. Узел перемещения данных используется только при передаче данных, в которой не участвует сервер (например, среда Network Data Management Protocol - NDMP). Средства перемещения данных выполняют обмен данными между устройствами хранения, не используя значительного количества ресурсов сервера, клиента или сети.
Сервер	Сервер, который управляется другим сервером IBM Spectrum Protect.

Администратор задает объекты хранения на логическом уровне сервера, как показано на Рис. 1.

Рис. 1. Объекты хранения



Дисковые устройства

Данные клиента можно хранить на дисковых устройствах со следующими типами томов:

- Каталоги в пулах хранения контейнеров каталогов
- Тома с произвольным доступом, относящиеся к типу устройств DISK
- Тома с последовательным доступом, относящиеся к типу устройств FILE

При использовании пулов хранения контейнеров каталогов для хранения данных IBM Spectrum Protect предлагает следующие возможности:

- Можно применить дедупликацию данных и методы кэширования диска, чтобы довести до максимума использование пространства для хранения данных.
- Данные с диска можно получать намного быстрее, чем из ленточного хранилища.

Физические ленточные устройства

В физической ленточной библиотеке емкость хранения определяется общим числом томов в бибиотеке. Физические ленточные устройства могут использоваться для следующих действий:

- Хранение резервных копий клиентских данных, клиентских архивных и перенесенных данных с клиентских узлов.
- Хранение резервных копий базы данных
- Экспорт данных на другой сервер или в хранилище вне площадки

Перемещение данных на ленту обеспечивает следующие преимущества:

- Можно сохранять данные для клиентов на дисковом устройстве одновременно с перемещением данных на ленту.
- Можно повысить производительность ленточного накопителя, производя перенос данных в потоке с диска на ленту.
- Можно распределить время использования накопителей, чтобы повысить эффективность ленточных накопителей.
- Можно перемещать данные на ленте во внесайтовые хранилища.
- Можно ограничить потребление мощности, так как ленточные устройства не потребляют питание после записи данных на ленту.
- Можно применить шифрование, обеспечиваемое аппаратными средствами ленточного накопителя, чтобы защитить данные на ленте.

По сравнению с эквивалентным хранилищем на дисках и виртуальным хранилищем на ленте себестоимость хранения единицы данных в случае физических ленточных устройств будет намного ниже.

Виртуальные ленточные библиотеки

Виртуальная ленточная библиотека (Virtual Tape Library, VTL) не использует физические ленточные носители. При использовании хранения VTL вы эмулируете механизмы доступа ленточного оборудования. В VTL можно задать тома и диски, чтобы обеспечить больше гибкости для среды хранения. Емкость хранения VTL определяется общим объемом доступного дискового пространства. Количество томов на диске и их объем можно увеличивать и уменьшать.

Если задать VTL на сервере IBM Spectrum Protect, при этом может повыситься производительность, так как сервер выполняет обработку точек монтирования для библиотек VTL иначе, чем для реальных ленточных библиотек. Хотя логические ограничения ленточных устройств все равно остаются, физические ограничения для ленточного оборудования неприменимы к VTL, обеспечивая более высокую масштабируемость. IBM Spectrum Protect VTL можно использовать, если выполнены следующие условия:

- В VTL эмулируется только один тип и поколение дисков и носителей.
- У каждого сервера и агента хранения с доступом к VTL есть пути, заданные для всех накопителей в библиотеке.

Хранение данных в пулах хранения

Основными компонентами в модели хранения данных IBM Spectrum Protect являются логические пулы хранения. Использование устройств хранения можно оптимизировать путем управления свойствами пулов хранения и томов.

Типы пулов хранения

Совокупность пулов хранения, заданных для сервера, называется *серверным хранилищем*. Можно задать в серверном хранилище следующие типы пулов хранения:

Первичные пулы хранения
: Именованный набор томов, которые сервер использует для хранения версий резервных копий файлов, архивных копий файлов и файлов, перенесенных с клиентских узлов.

Пулы хранения копий
: Именованный набор томов, содержащих копии файлов из первичного пула хранения. Пулы хранения копий используются только для резервного копирования данных, находящихся в первичных пулах хранения. Пул хранения копий может быть пунктом назначения для группы резервных копий, группы архивных копий или класса управления для файлов с управлением пространством.

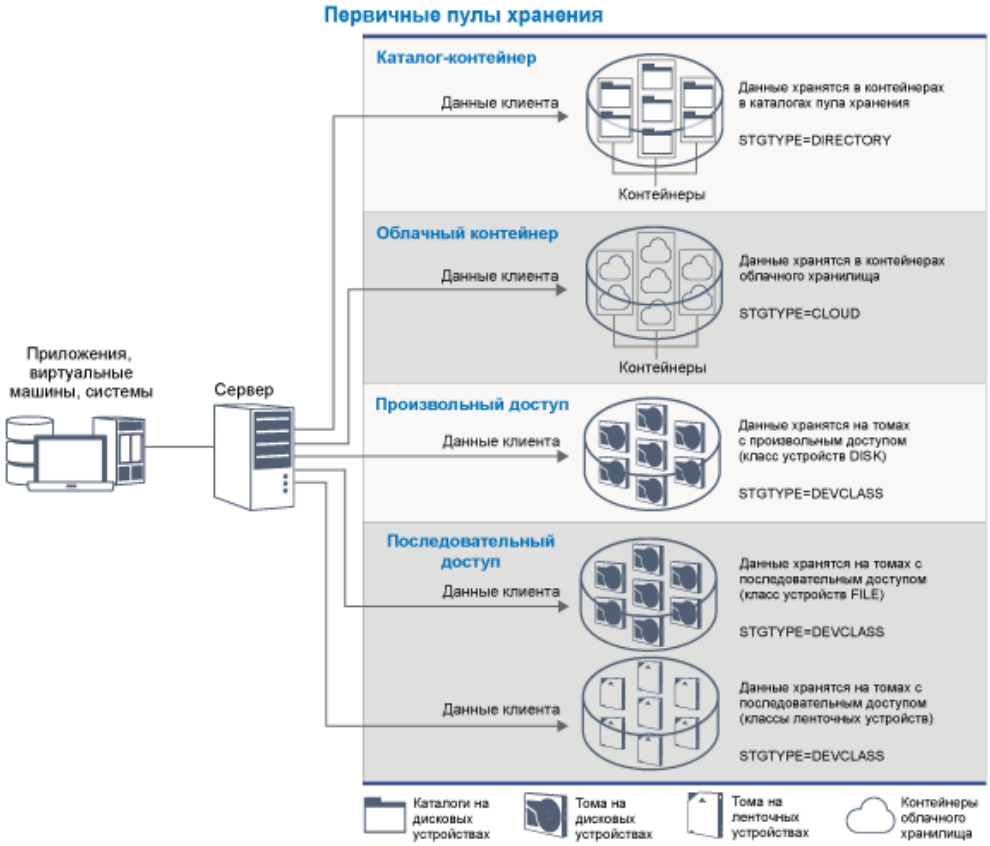
Пулы хранения контейнера-копии
: Именованный набор томов, содержащих копию экстентов данных, находящихся в пулах хранения каталогов-контейнеров. Пулы хранения копий используются только для защиты данных, находящихся в пулах хранения каталогов-контейнеров.

Пулы хранения активных данных
: Именованный набор томов хранения, содержащий только активные резервные версии клиентских данных.

Первичные пулы хранения

При восстановлении, получении, возврате или экспорте файла данных затребованный файл берется из первичного пула хранения. В зависимости от типа первичного пула хранения пулы хранения данных могут находиться на площадке или вне площадки. Первичные пулы хранения можно организовать в виде иерархии хранения, чтобы данные можно было переносить из дискового пространства хранения в более экономичное пространство хранение, например, на ленточные устройства. На Рис. 1 проиллюстрировано понятие первичных пулов хранения.

Рис. 1. Первичные пулы хранения



Можно задать следующие типы первичных пулов хранения:

Пулы хранения контейнеров каталогов
: Пул хранения, используемый сервером для хранения данных в контейнерах в каталогах облачного пула. Данные, хранящиеся в пуле хранения каталогов-контейнеров, могут использовать либо встроенную дедупликацию данных, либо дедупликацию данных на стороне клиента, либо встроенное сжатие, либо сжатие на стороне клиента. Встроенная дедупликация данных или встроенное сжатие сокращают объем данных при их хранении.

Совет: Данные, которые сначала сжали, невозможно дедуплицировать, однако, дедуплицированные данные можно сжать.

Используя пулы хранения каталогов-контейнеров, вы избавляетесь от необходимости исправления томов, за счет чего повышается производительность сервера и снижается стоимость оборудования хранения. Данные в пулах хранения каталогов-контейнеров можно защищать и исправлять на уровне пула хранения. Данные, хранящиеся в пуле хранения каталогов-контейнеров, можно разбить на слои, переместив их в пул хранения облачного контейнера.

Ограничение: Вместе с пулами хранения каталогов-контейнеров нельзя использовать ни одну из перечисленных ниже функций:

- Перенос
- Освобождение пространства
- Агрегирование
- Совместное размещение
- Одновременная запись
- Резервное копирование пула хранения
- Виртуальные тома

Пулы хранения облачных контейнеров

Пул хранения, используемый сервером для хранения данных в облачном пространстве хранения. Облачное пространство хранения может находиться на месте или вне системы. Пулы хранения облачных контейнеров, которые обеспечивает IBM Spectrum Protect, позволяют хранить данные в облачном пространстве хранения на основе объектов. Сохраняя данные в пулах хранения облачных контейнеров, можно использовать преимущества более низкой стоимости за единицу, которые предлагает облако, вместе с возможностями масштабирования, обеспечиваемыми хранением в облаке. Разбиение на слои в облаке можно использовать, чтобы снизить стоимость, перемещая данные из дискового хранилища в пул хранения облачного контейнера. IBM Spectrum Protect управляет учетными данными, защитой, вводом-выводом для чтения и записи, а также жизненным циклом данных, хранящихся в облаке. Когда на сервере реализуются пулы хранения облачных контейнеров, вы можете записывать данные непосредственно в облако, сконфигурировав пул хранения облачных контейнеров с использованием облачных учетных данных. Данные, хранящиеся в пуле хранения облачных контейнеров, используют и встроенную дедупликацию данных, и встроенное сжатие. Сервер записывает дедуплицированные, сжатые и зашифрованные данные непосредственно в облако. Вы можете производить резервное копирование данных и восстанавливать данные или архивировать и получать данные непосредственно из пула хранения облачных контейнеров.

Можно задать следующие типы пулов хранения облачных контейнеров:

На месте
: Тип хранения На месте позволяет хранить данные в частном облаке, что обеспечивает более сильную защиту и максимальный контроль за данными. Недостатками частного облака являются более высокая стоимость из-за требований к аппаратным средствам и обслуживанию на месте.

Вне системы
: Тип хранения Вне системы для пула хранения на основе облачного контейнера позволяет хранить данные в общедоступном облаке. Преимуществом использования общедоступного облака является то, что вы сможете достичь более низкой стоимости, чем в случае частного облака, например, за счет устранения обслуживания. Однако вы должны сбалансировать это преимущество с возможными проблемами, влияющими на производительность, из-за скоростей соединения и сокращения возможностей управления вашими данными.

Пулы хранения, связанные с классами устройств
: Вы можете задать первичный пул хранения, чтобы использовать следующие типы устройств хранения:

Класс устройств DISK
: В случае типа устройств DISK в пуле хранения данные хранятся в дисковых блоках с произвольным доступом. Можно использовать кэширование в пулах хранения DISK, чтобы повысить производительность восстановления клиента при некоторых ограничениях по обработке на сервере. Распределение пространства и отслеживание по блокам требует больше пространства для хранения в базе данных и больше вычислительных ресурсов, чем распределение и отслеживание по томам.

Класс устройств FILE
: В случае типа устройств FILE в пуле хранения файлы хранятся на последовательных томах, чтобы обеспечить более высокую производительность последовательного доступа, чем при хранении на дисковых блоках. Для сервера эти файлы будут иметь характеристики ленточного тома, поэтому такой тип пула хранения лучше

подходит для переноса на ленту. Тома FILE полезны как *электронное хранилище*, когда данные передаются на удаленную площадку по электронной сети, а не путем физической поставки ленты. В общем случае, этот тип пула хранения является более предпочтительным, чем пулы хранения DISK.

У сервера есть следующие первичные пулы хранения с произвольным доступом по умолчанию:

ARCHIVEPOOL
: В политике STANDARD этот пул хранения является пунктом назначения для файлов, создаваемых в качестве архивов с клиентских узлов.

BACKUPPOOL
: В политике STANDARD этот пул хранения является пунктом назначения для файлов, создаваемых в качестве резервных копий с клиентских узлов.

SPACEMGPOOL
: Этот пул хранения предназначен для HSM-управляемых файлов, перенесенных с клиентских узлов IBM Spectrum Protect for Space Management.

Пулы хранения копий

В пулах хранения копий содержатся активные и неактивные версии данных, резервные копии которых были созданы на основе данных в первичных пулах хранения. Пул хранения каталога-контейнера нельзя использовать как пул хранения копий. Кроме того, данные из пула хранения каталога-контейнера нельзя скопировать в пул хранения копий. Для защиты пулов хранения каталогов-контейнеров скопируйте данные в пул хранения контейнеров-копий. На Рис. 2 проиллюстрировано понятие пулов хранения копий.
Рис. 2. Пулы хранения копий

Пулы хранения копий представляют собой средство восстановления после аварий или сбоев носителей. Например, если клиент пытается получить поврежденный файл из первичного пула хранения, а пул хранения недоступен или файл в пуле хранения поврежден, клиент может восстановить данные из пула хранения копий.

Тома пулов хранения копий можно переместить вне системы, при этом сервер все равно будет отслеживать эти тома. Перемещение этих томов обеспечивает возможность восстановления после аварии на месте. Пул хранения копий может использовать только пространство хранения с последовательным доступом, например, класс ленточных устройств или класс устройств FILE.

Пулы хранения контейнера-копии

Сервер может защитить пул хранения каталогов-контейнеров, сохраняя копии данных в пулах хранения контейнеров-копий. Данные в пулах хранения контейнеров-копий хранятся на ленточных томах, которые могут быть сохранены локально или дистанционно. Поврежденные данные в пулах хранения каталогов-контейнеров можно восстановить при помощи дедуплицированных экстентов в пулах хранения контейнеров-копий. Пулы хранения контейнеров-копий - это альтернатива использованию сервера репликации для защиты данных в пуле хранения каталогов-контейнеров.

Ограничение: Если все серверные данные потеряны, то одни только пулы хранения контейнеров-копий не обеспечат такой же уровень защиты, как репликация:

- С помощью репликации можно восстанавливать данные клиента непосредственно с сервера назначения, если исходный сервер недоступен.
- Работая с пулами хранения контейнеров-копий, надо сначала восстановить сервер из резервной копии базы данных и затем исправить пулы хранения каталогов-контейнеров с ленточных устройств.

На Рис. 3 проиллюстрировано понятие пулов хранения контейнеров-копий.

Рис. 3. Пулы хранения контейнера-копии

В зависимости от конфигурации вашей системы, можно создать расписания защиты для одновременного копирования данных пула хранения каталогов-контейнеров в локальные или удаленные пулы хранения контейнеров-копий для соответствия вашим требованиям:

- Если репликация включена, можно создать один пул контейнеров-копий вне узла. Дистанционная копия может использоваться для обеспечения дополнительной защиты в реплицированной среде.
- Если репликация выключена, можно создать один пул хранения контейнеров-копий на узле и один - вне узла.

В зависимости от ресурсов и требований вашего сайта, возможность копирования пулов хранения каталогов-контейнеров на ленту дает следующие выгоды:

- Избавляет вас от поддержки других серверов и дает больше пространства хранения на диске.
- Данные копируются в пулы хранения, заданные на сервере. При этом сетевое соединение между серверами никак не влияет на производительность.
- Для копирования на удаленные ленты надо соответствовать всем нормативным и деловым требованиям.

Пулы хранения активных данных

В пуле активных данных содержатся только активные версии резервных копий клиентских данных. В этом случае серверу не нужно находить неактивные файлы, которые не надо восстанавливать. Пул хранения каталога-контейнера нельзя использовать как пул хранения активных данных. Пулы активных данных используются, чтобы повысить эффективность операций хранения и восстановления. Например, этот тип пула хранения может помочь вам достичь следующих целей:

- Повысить скорость операций восстановления данных клиента
- Сократить число томов хранения на месте или вне системы
- Сократить объем данных, передаваемых при копировании или восстановлении файлов, хранящихся в электронном виде на удаленной площадке

В пулах активных данных не могут находиться файлы, перенесенные клиентами управления иерархическим хранилищем, равно как и архивные файлы. Поскольку обновленные версии резервных копий данных хранятся в пулах активных данных, более старые версии удаляются, так как оставшиеся данные консолидируются с многих томов с последовательным доступом на меньшее число новых томов с последовательным доступом. На Рис. 4 проиллюстрировано понятие пулов хранения активных данных.

Рис. 4. Пулы хранения активных данных

Для создания пулов активных данных можно использовать любые типы пространства хранения с последовательным доступом. Однако преимущества пула активных данных зависят от типа устройств, связанного с пулом. Например, для

операций быстрого восстановления клиентах идеально подходят пулы активных данных, связанные с классом устройств FILE, по следующим причинам:

- Тома FILE не нужно физически монтировать
- Сеансы клиентов, восстанавливающиеся с томов типа FILE в пуле активных данных, могут получить доступ к томам одновременно, что повышает производительность восстановления.

Информация, связанная с данной:

Часто задаваемые вопросы о пулах хранения каталогов-контейнеров

Часто задаваемые вопросы о пулах хранения облачных контейнеров

Транспорт данных в пространство хранения в разных сетях

Среда IBM Spectrum Protect обеспечивает возможности безопасного перемещения данных в пространство хранения по разным типам сетей и при разных конфигурациях.

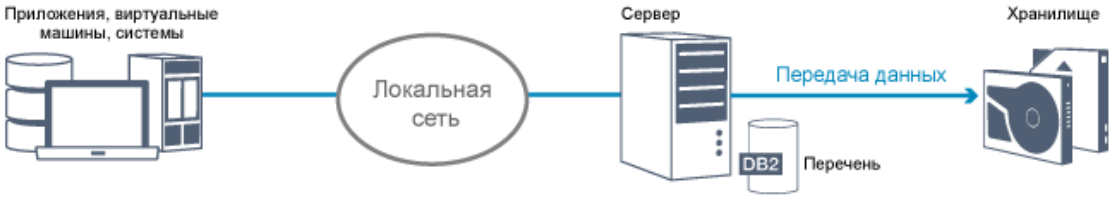
Конфигурации сети для устройств хранения

IBM Spectrum Protect обеспечивает методы конфигурирования клиентов и серверов в локальной сети (local area network, LAN), в сети хранения данных (storage area network, SAN), перемещения данных без локальной сети и использования подключенного к сети хранилища (network-attached storage, NAS).

Операции резервного копирования данных через LAN

На Рис. 1 показан путь данных для операций резервного копирования IBM Spectrum Protect через LAN.

Рис. 1. Операции резервного копирования IBM Spectrum Protect через LAN

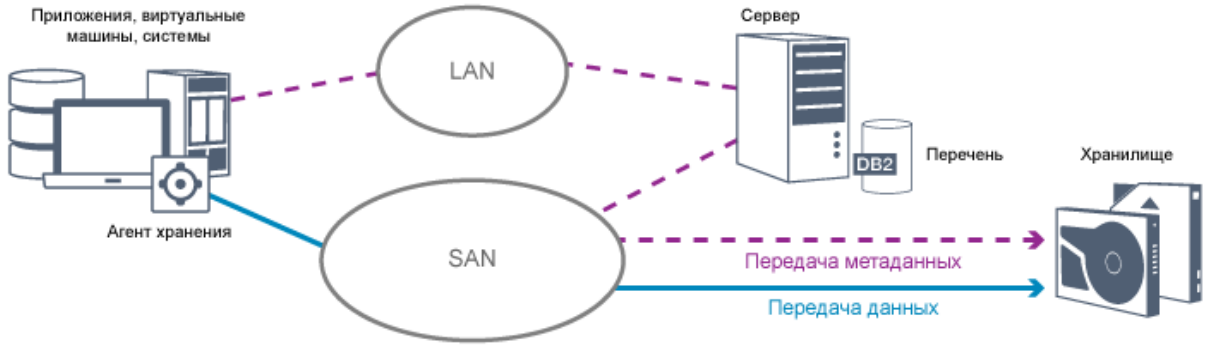


В конфигурации LAN одна или несколько ленточных библиотек связаны с одним сервером IBM Spectrum Protect. При таком типе конфигурации клиентские данные, электронная почта, терминальные подключения, программа и информация для управления устройствами должны обслуживаться одной и той же сетью. Информация для управления устройством и клиентские данные резервного копирования и восстановления передаются по локальной сети.

Операции резервного копирования данных через SAN

На Рис. 2 показан путь данных для операций резервного копирования IBM Spectrum Protect через SAN.

Рис. 2. Операции резервного копирования IBM Spectrum Protect через SAN



Сеть хранения данных (SAN) - это выделенная сеть хранения, которая может дать выигрыш в производительности системы. В сети SAN можно объединить хранилище и преодолеть ограничения на расстояние, масштабируемость и пропускную способность локальных и глобальных сетей. Применяя IBM Spectrum Protect в SAN, можно воспользоваться преимуществами следующих функций:

- Совместное использование устройств хранения несколькими серверами IBM Spectrum Protect. Устройства, использующие тип устройств GENERICTAPE, не включаются.

- Переместите данные из системы клиента непосредственно на устройства хранения, не используя локальную сеть. Перемещение данных в режиме без локальной сети требует установки агента хранения на клиентской системе. Агент хранения прилагается к продукту IBM Spectrum Protect for SAN.

  С помощью агента хранения клиент может напрямую производить резервное копирование и восстановление данных в ленточную библиотеку или в такую совместно используемую файловую систему, как GPFS. Сервер IBM Spectrum Protect обслуживает базу данных и журнал восстановления сервера и выступает в роли менеджера библиотек для управления операциями устройств. Агент хранения на клиенте обрабатывает перенос данных на устройство в сети SAN. Благодаря этой реализации высвобождается ширина полосы пропускания в локальной сети (LAN), которая в противном случае применялась бы для перемещения данных клиента.

- Совместное использование ленточных носителей и библиотек, поддерживаемых сервером IBM Spectrum Protect.
- Использование единого имени клиентского узла для нескольких клиентов в общей параллельной файловой системе (кластер GPFS).

Хранилище NAS
: Файл-серверы NAS — это выделенные серверы для хранения, операционные системы на которых оптимизированы для выполнения функций по обслуживанию файлов.. Файл-серверы NAS, как правило, взаимодействуют с IBM Spectrum Protect через такие сетевые протоколы промышленного стандарта, как сетевой протокол управления данными (network data management protocol, NDMP), или через основное хранилище для пулов хранения с произвольным доступом или последовательным доступом. В IBM Spectrum Protect есть следующдие основные типы конфигураций, в которых используется NDMP для операций резервного копирования и управления файл-серверами NAS:

  - IBM Spectrum Protect создает резервную копию файл-сервера NAS на библиотечном устройстве, непосредственно подключенном к файл-серверу NAS. Файл-сервер NAS, который может быть удаленным по отношению к серверу IBM Spectrum Protect, передает резервные копии данных непосредственно на накопитель в ленточную библиотеку, подключенную к SCSI. Данные сохраняются в сформатированных под NDMP пулах хранения, которые могут быть скопированы на носители для хранения, которые в свою очередь можно переместить в дистанционное хранилище для защиты в случае аварии на узле.
  - IBM Spectrum Protect создает резервную копию файл-сервера NAS по локальной сети в иерархии пулов хранения. При таком типе конфигурации данные можно сохранять непосредственно на диске с произвольным либо последовательным доступом, а затем переносить на ленту. Этот тип конфигурации также можно использовать для репликации систем. Также можно выполнять резервное копирование данных на носители хранения, которые можно переместить в удаленное положение (вне системы). Преимуществом этого типа конфигурации является то, что у вас есть все функции управления данными, связанные с иерархией пулов хранения.
  - Клиент IBM Spectrum Protect читает данные из системы NAS, используя протоколы NFS или CIFS, и отправляет данные на сервер для хранения.

Управление хранением

Вы управляете устройствами и носителями, которые используются для хранения клиентских данных, через сервер IBM Spectrum Protect. Сервер объединяет управление хранением с политиками, которые вы задаете для управления клиентскими данными в следующих областях:

Типы устройств для серверного хранилища
: При работе с IBM Spectrum Protect для системы хранения сервера можно использовать непосредственно подключенные устройства и устройства, подключенные к сети. IBM Spectrum Protect представляет физические устройства хранения и носители с объектами, определяемыми администратором.

Перенос данных в иерархии хранения
: В случае первичных пулов хранения, не являющихся пулами хранения контейнеров каталогов, можно организовать пулы хранения в одну или несколько иерархических структур. Эта иерархия хранения обеспечивает гибкость разными способами. Например, можно задать политику, чтобы производить резервное копирование данных на диски для выполнения более быстрых операций резервного копирования. Сервер IBM Spectrum Protect может затем автоматически переносить данные с диска на ленту.

Удаление устаревших данных
: Заданная политика определяет, когда должен заканчиваться срок хранения данных на сервере IBM Spectrum Protect. Для удаления данных с истекшим сроком хранения серверный процесс помечает их как данные, срок хранения которых истек, и удаляет из базы данных соответствующие метаданные. Теперь место, которое занимали

такие данные, доступно для хранения новых данных. Вы можете управлять частотой выполнения процесса обработки данных с истекшим сроком хранения, используя соответствующую серверную опцию.

Повторное использование носителей за счет их освобождения

Серверные политики автоматически завершают срок хранения данных, поэтому на носителях, на которых хранятся эти данные, остается свободное место. В случае носителей хранения, не являющихся пулами хранения контейнеров каталогов или пулами хранения дисков с произвольным доступом, сервер IBM Spectrum Protect реализует *рекламацию* (высвобождение) - процесс, который высвобождает носитель для повторного использования без традиционной перемотки ленты. В процессе высвобождения происходит автоматическая дефрагментация путем консолидации данных, период хранения которых не истек, на других носителях, когда размер свободного места на носителях достигает заданного уровня. После этого сервер может повторно использовать освобожденные носители. Консолидация позволяет производить автоматическую рециркуляцию носителя через процесс управления хранением и сводить к минимуму число необходимых носителей.

Консолидация резервных копий данных клиента

Группируя данные клиента, для которых созданы резервные копии, можно сести к минимуму число монтирований носителей, необходимых для восстановления клиента. Сервер IBM Spectrum Protect обеспечивает следующие методы группировки файлов клиентов на носителях хранения, отличающихся от пулов хранения контейнеров каталогов:

Совместное размещение данных клиентов

Сервер IBM Spectrum Protect может *совместно размещать* данные клиента, другими словами, данные клиента хранятся на нескольких томах, а не распределяются по многим томам. Совместное размещение по клиентам сводит к минимуму число томов, необходимых для резервного копирования и восстановления данных клиентов. Совместное размещение данных может повысить число монтирований томов, так как каждому клиенту может потребоваться выделенный том вместо того, чтобы данные с нескольких клиентов хранились на одном и том же томе.

Можно настроить сервер для совместного размещения клиентских данных, когда данные изначально помещаются в серверное хранилище. В иерархии хранения можно совместное размещать данные при их переносе сервером из исходного пула хранения в следующий пул хранения в иерархии хранения. Совместное размещение можно выполнить по клиентам или по группам клиентов. Выбор зависит от размера хранящихся файловых пространств и требований к восстановлению.

Связывание пулов активных данных с различными устройствами

Пулы активных данных полезны для быстрого восстановления данных клиента. Преимуществом является сокращение числа локальных или удаленных томов хранения или уменьшение полосы пропускания при копировании или восстановлении файлов, хранящихся в удаленной системе. Пулы активных данных, в которых используются сменные носители, например, ленточные, обладают сходными преимуществами. Хотя ленточные устройства необходимо монтировать, серверу не приходится осуществлять их перемотку до конца массива данных, содержащего старые неактивные файлы. Однако основным преимуществом использования сменных носителей в пулах активных данных является сокращение числа томов, используемых для хранения данных на месте и вне системы. Если вы храните данные на удаленной площадке, вы можете свести к минимуму объем данных, которые нужно передавать, копируя и восстанавливая только активные данные.

Создание набора резервных копий

Набор резервных копий содержит все активные резервные копии файлов, существующие в серверном хранилище для данного клиента. Набор резервных копий размещается на сменных носителях и сохраняется в течение заданного периода времени. Набор резервных копий является дополнением к уже сохраненным резервным копиям, и для него требуются дополнительные носители.

Перемещение данных на клиентский узел

Данные клиентского узла можно объединить, переместив их в пределах серверного хранилища. Можно переместить набор резервных копий на другой носитель, где набор резервных копий будет храниться до заданного вами времени. Объединение данных может повысить эффективность во время выполнения операций восстановления или извлечения в клиенте.

Стратегии защиты данных с использованием IBM Spectrum Protect

IBM Spectrum Protect обеспечивает возможность реализовать различные стратегии защиты данных.

IBM Spectrum Protect можно сконфигурировать для отправки данных на устройства хранения, которые находятся на локальной площадке или на удаленной площадке. Чтобы довести до максимума защиту данных, можно сконфигурировать репликацию на удаленный сервер.

- Стратегии минимизации использования пространства хранения для резервных копий
  Чтобы свести к минимуму необходимый объем пространства хранения, IBM Spectrum Protect создает резервные копии данных, используя дедупликацию данных и метод прогрессивного инкрементного резервного копирования.
- Стратегии для защиты при авариях
  IBM Spectrum Protect обеспечивает стратегии для защиты данных в случае аварии. Эти стратегии включают репликацию узлов на удаленную площадку, защиту пулов хранения, резервное копирование базы данных, перемещение лент с резервными копиями вне сайта и репликацию устройств на сервере ожидания.
- Стратегии для аварийного восстановления с использованием IBM Spectrum Protect
  IBM Spectrum Protect обеспечивает несколько путей восстановления сервера, если произойдет отказ базы данных или пулов хранения.

Стратегии минимизации использования пространства хранения для резервных копий

Чтобы свести к минимуму необходимый объем пространства хранения, IBM Spectrum Protect создает резервные копии данных, используя дедупликацию данных и метод прогрессивного инкрементного резервного копирования.

Дедупликация данных

Когда сервер IBM Spectrum Protect получает данные с клиента, сервер идентифицирует дубликаты экстентов данных и сохраняет уникальные экземпляры экстентов данных в пуле хранения каталога-контейнера. Метод дедупликации данных улучшает использование пространства хранения и устраняет необходимость в выделенном устройстве для дедупликации данных.

Рис. 1. Процесс дедупликации данных

Если много раз встречается один и тот же байтовый шаблон, дедупликация данных существенно сократить объем данных, которые нужно сохранить или передать. Помимо целых файлов IBM Spectrum Protect также может выполнять дедупликацию частей файлов, совпадающих с частями других файлов.

IBM Spectrum Protect обеспечивает следующие типы дедупликации данных:

Дедупликация данных на стороне сервера
: Сервер выявляет дубликаты экстентов данных и перемещает данные в пул хранения каталога-контейнера. Процесс на стороне сервера использует *встроенную дедупликацию данных*, при которой данные дедуплицируются одновременно с их записью в пул хранения каталога-контейнера. Дедуплицированные данные также могут хранится в пулах хранения других типов. Встроенная дедупликация данных на сервер обеспечивает следующие преимущества:

  - Устраняется необходимость в высвобождении пространства
  - Сокращается объем пространства, занятого хранящимися данными

Дедупликация данных на стороне клиента

При таком методе обработка распределяется между сервером и клиентом в процессе резервного копирования. Клиент и сервер определяют и удаляют дубликаты данных, чтобы сэкономить пространство хранения на сервере. При дедупликации данных на стороне клиента на сервер отправляются только сжатые и дедуплицированные данные. Сервер хранит данные в сжатом формате, обеспечиваемом клиентом. Дедупликация данных на стороне клиента обеспечивает следующие преимущества:

- Сокращается объем данных, передаваемых по локальной сети (LAN).
- Устраняются лишние затраты мощностей на обработку и сокращается время, необходимое для удаления дубликатов данных на сервере
- Повышается производительность базы данных, так как дедупликация данных на стороне клиента также является встроенной

Вы можете комбинировать дедупликацию данных на стороне клиента и дедупликацию данных на стороне сервера в одной и той же производственной среде. Возможность производить дедупликацию на клиенте или на сервере обеспечивает гибкость использования ресурсов, управления политикой и защитой данных.

Сжатие

Используйте встроенное сжатие, чтобы сократить объем пространства в пулах хранения контейнеров. Данные сжимаются при их записи в пул хранения контейнера.
Ограничение: Сервер IBM Spectrum Protect не может сжимать зашифрованные данные.

Прогрессивное инкрементное резервное копирование

В процессе прогрессивного инкрементного резервного копирования сервер осуществляет мониторинг операций клиента и создает резервные копии всех файлов, которые изменились после первоначального полного резервного копирования. Производится резервное копирование всех файлов, так что серверу не нужно обращаться к базовым версиям файлов. Этот метод резервного копирования устраняет необходимость наличия нескольких полных резервных копий данных клиента, тем самым позволяя сэкономить сетевые ресурсы и пространство хранения.

Стратегии для защиты при авариях

IBM Spectrum Protect обеспечивает стратегии для защиты данных в случае аварии. Эти стратегии включают репликацию узлов на удаленную площадку, защиту пулов хранения, резервное копирование базы данных, перемещение лент с резервными копиями вне сайта и репликацию устройств на сервере ожидания.

Репликация на удаленной площадке

Репликация узлов - это процесс инкрементного копирования данных с одного сервера на другой. Сервер, с которого реплицируются данные клиента, называется *исходным сервером репликации*. Сервер, на который реплицируются данные клиента, называется *целевым сервером репликации*. В целях защиты от аварий сервер репликации назначения находится на удаленном сайте. Сервер репликации может работать как исходный сервер и/или как целевой сервер. Вы используете репликацию, чтобы поддерживать одно и то же число версий файлов на исходном и целевом сервере репликации.

Репликация узла обеспечивает немедленную дорступность данных за счет передачи управления при отказе. Хотя репликация узлов защищает большую часть метаданных, этот подход не обеспечивает адекватную защиту на случай повреждения базы данных. Можно обеспечить более сложную защиту, используя пулы хранения для хранения резервных копий данных.

Преимущества

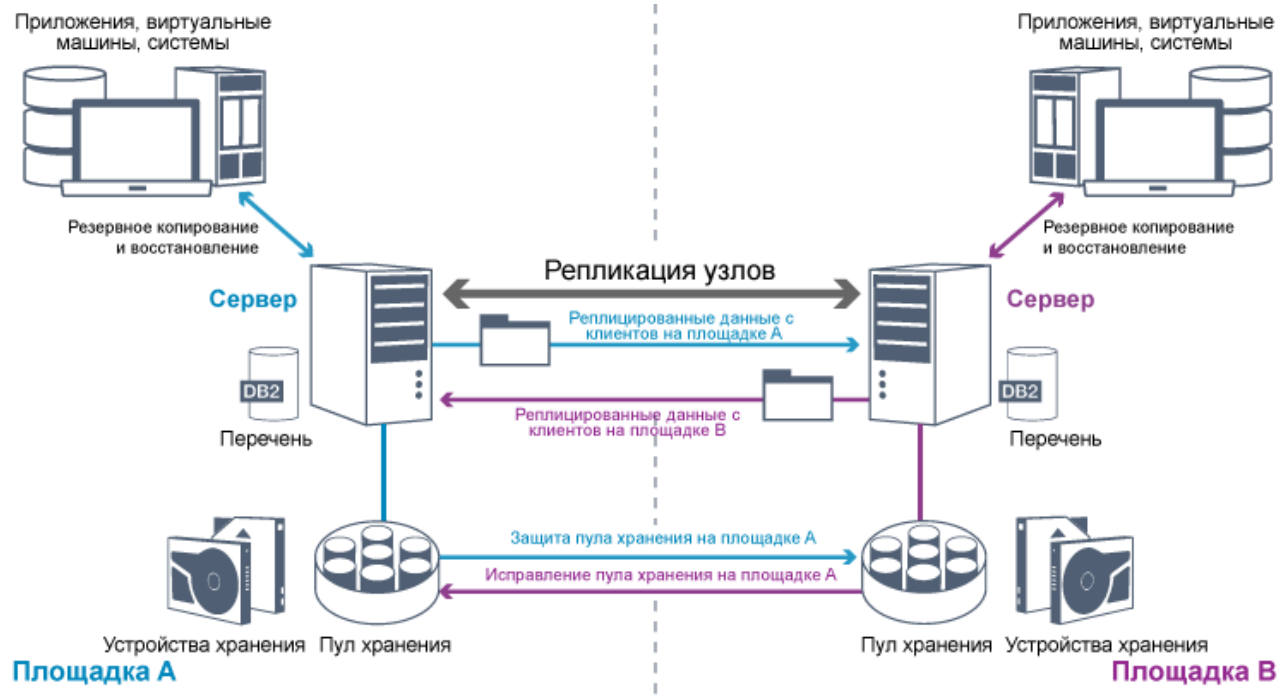
- Отказоустойчивость, благодаря которой данные становятся доступны немедленно, если произойдет авария.
- Инкрементная репликация, которая обеспечивает быструю передачу данных.
- Электронная передача
- Защита и данных, и большинства метаданных

Недостатки

- Нужно восстанавливать как данные, так и метаданные.
- Данные на исходном сервере нужно снова реплицировать с удаленной площадки.

На Рис. 1 показан процесс репликации узла на удаленной площадке.

Рис. 1. Процесс репликации узла



При репликации данных клиента на целевой сервер копируются данные, которых нет на целевом сервере. Когда объем реплицированных данных превысит предел хранения, целевой сервер автоматически удалит данные с исходного сервера. Чтобы получить максимальный эффект с точки зрения защиты данных, вы синхронизируете локальный сервер и удаленный сервер; например, площадка B реплицирует данные с площадки A, а площадка A реплицирует даные с площадки B. В ходе обработки репликации с целевого сервера также удаляются данные клиента, которые были удалены с исходного сервера.

IBM Spectrum Protect обеспечивает следующие функции репликации:

- Вы можете задать политики для целевого сервера следующими способами:
  - Идентичные политики на исходном сервере и на целевом сервере
  - Разные политики на исходном сервере и на целевом сервере, соответствующие разным бизнес-требованиям.

  Если произойдет авария и исходный сервер окажется недоступен, клиенты смогут восстановить данные с целевого сервера. Если исходный сервер восстановить невозможно, вы можете направить клиенты для сохранения данных на целевом сервере. В случае перебоя с питанием клиента, которые производили резервное копирование на исходный сервер, смогут автоматически передать управление для восстановления данных с сервера назначения (целевого сервера).
- Вы можете использовать обработку репликации для восстановления поврежденных файлов из пулов хранения. Нужно реплицировать данные клиента на целевом сервера до повреждения файлов. Последующие процессы репликации обнаруживают поврежденные файлы на исходном сервере и заменяют файлы неповрежденными файлами с целевого сервера.

Роль репликации в защите в случае аварии

Если произойдет авария, вы сможете восстановить реплицированные данные с удаленной площадки и поддерживать один и тот же уровень файлов на исходном и целевом серверах. Вы используете репликацию для достижения следующих целей:

- Управление пропускной способностью сети при планировании репликации узлов в заданное время
- Восстановление данных после потери площадки.
- Восстановление поврежденных файлов на исходном сервере.

Защита пула хранения

Как часть стратегии аварийного восстановления, убедитесь, что резервная копия данных в пулах хранения доступна на удаленной площадке.

Преимущества

- Быстрое восстановление и перестройка исходной системы.

Недостатки

- Защищаются только данные. метаданные не защищаются.
- Для каждого пула хранения необходимо задать носитель хранения.

Для защиты от необратимой потери данных, хранящихся в пулах хранения контейнеров и в пулах хранения FILE и DISK, используются различные методы.

Пулы хранения контейнеров каталогов

Если вам не нужно реплицировать все данные, содержащиеся на узле клиента, вы используете пулы хранения копий для защиты некоторых пулов хранения каталогов-контейнеров. Защищая пул хранения контейнеров каталогов, вы не используете ресурсы, которые реплицируют существующие данные и метаданные, что позволяет повысить производительность сервера.

Предпочтительный метод заключается в защите пула хранения каталогов-контейнеров перед репликацией клиентского узла. При запуске репликации узла экстенты данных, которые уже были реплицированы за счет защиты пула хранения, будут пропущены, что сокращает время обработки репликации. Если данные в пуле хранения каталога-контейнера окажутся повреждены, вы сможете восстановить данные из копии в пуле хранения контейнера-копии.

Пулы хранения контейнера-копии

Вы защищаете пулы хранения каталогов-контейнеров, копируя данные в пуле хранения каталога-контейнера в пулы хранения контейнеров-копий. Пулы хранения контейнеров-копий позволяют создать до двух ленточных копий пула хранения каталогов-контейнеров. Ленточные копии могут быть сохранятья локально или дистанционно. Поврежденные данные в пулах хранения каталогов-контейнеров можно восстановить при помощи пулов хранения контейнеров-копий. Пулы хранения контейнеров-копий - это альтернатива использованию сервера репликации для защиты данных в пуле хранения каталогов-контейнеров.

Пулы хранения, связанные с классами устройств FILE и DISK

Для пулов хранения, связанных с классами устройств FILE и DISK, вы используете репликацию узлов, чтобы сохранять непротиворечивую копию узла для данных на целевом сервере. Копию данных можно непосредственно восстановить с целевого сервера в пулы хранения.

Резервные копии базы данных

Вы используете резервные копии базы данных для восстановления системы после повреждения базы данных. Кроме того, нужно использовать операции резервного копирования базы данных, чтобы не дать DB2 исчерпать пространство архивного журнала. Операции резервного копирования базы данных не являются частью репликации узлов. Резервные копии базы данных могут содержать полные или инкрементные резервные копии, а также копии, выполненные в режиме снимка. Чтобы обеспечить возможность аварийного восстановления, нужно хранить резервные копии базы данных вне сайта. Для восстановления базы данных необходимы тома резервных копий базы данных. Вы можете восстановить базу данных с томов резервных копий либо путем восстановления моментального снимка, либо с помощью операции самого актуального восстановления.

Восстановление на заданный момент времени

Используйте операции восстановления на момент времени в таких ситуациях, как аварийное восстановление, или для устранения последствий ошибок, которые могут вызвать противоречия в базе данных. Операции восстановления для базы данных, которые используют резервные копии моментальных снимков, являются разновидностью операции восстановления на заданный момент времени. Операция восстановления на заданный момент времени включает в себя следующие действия:

- Удаляется и создается заново каталог активного журнала и каталог архивного журнала, заданные в файле dsmserv.opt.
- Образ базы данных восстанавливается с томов резервных копий в каталоги базы данных, записанные в резервной копии базы данных, или в новые каталоги.
- Архивные журналы восстанавливаются с томов резервных копий, находящихся в хранилище переполнения.
- Используется информация журналов из каталога переполнения вплоть до заданного момента времени.

Восстановление до самого последнего состояния

Если нужно восстановить базу данных на момент, когда она была потеряна, восстановите ее до наиболее актуального состояния. Операция восстановления до самого последнего состояния включает в себя следующие действия:

- Образ базы данных восстанавливается с томов резервных копий в каталоги базы данных, записанные в резервной копии базы данных, или в новые каталоги.
- Архивные журналы восстанавливаются с томов резервных копий, находящихся в хранилище переполнения.
- Используется информация журналов из каталога переполнения и архивных журналов из каталога архивного журнала.

Самое последнее восстановление не удаляет и не создает заново каталог активного журнала и каталог архивного журнала.

Альтернативные методы защиты от аварий

Помимо репликации, защиты пулов хранения и резервного копирования базы данных для защиты данных и реализации аварийного восстановления с использованием IBM Spectrum Protect также можно использовать следующие методы:

Отправка лент с резервными копиями на удаленную площадку
: Резервные копии данных создаются на ленте исходным сервером в запланированное время. Ленты отправляются на удаленную площадку. Если произойдет авария, ленты будут возвращены на площадку исходного сервера и данные будут восстановлены на исходных клиентах. Копии данных вне площадки на ленте с резервными копиями также могут помочь вам произвести восстановление после атак злонамеренных программ.

Репликация устройств с несколькими площадками на резервный сервер
: В конфигурации устройств с несколькими площадками исходное устройство реплицируется на удаленный сервер в архитектуре SAN. При такой конфигурации, если оборудование клиента на исходной площадке повреждено, исходное устройство можно реплицировать с резервного сервера на удаленной площадке. Эта конфигурация обеспечивает возможность выполнения операции резервного копирования и восстановления на основе дисков.

Сравнение стратегий конфигурации защиты

Рассмотрим следующие возможные сценарии потери данных:

- Данные базы данных повреждены: защита от потери данных в базе данных с использованием резервной копии базы данных на площадке.
- Данные пулов хранения повреждены: защита от потери данных в пулах хранения с использованием копии пулов хранения на площадке или репликации узлов.
- Сценарий аварийного восстановления, когда оказались потеряны и база данных на площадке, и пулы хранения: вы защищаетесь от всеобъемлющей аварии, используя репликацию узлов и как резервную копию базы данных вне площадки, так и резервные копии пула хранения.

При наиболее распространенных сценариях защиты данных решением будут следующие возможные конфигурации:

Конфигурации только для защиты от повреждений

- Реализуйте операции резервного копирования базы данных на сайте, используя дополнительный пул хранения контейнера-копии на площадке для защиты данных в пулах хранения каталогов-контейнеров.
- Реализуйте операции резервного копирования базы данных на площадке и репликацию узлов на площадке.

Конфигурации для восстановления после аварий и защиты от повреждений

- Реализуйте операции резервного копирования базы данных вне сайта с использованием пулов хранения контейнеров-копий, чтобы защитить данные в пулах хранения каталогов-контейнеров.
- Реализуйте операции резервного копирования базы данных на сайте и репликацию узлов вне сайта, используя дополнительный пул хранения контейнера-копии на площадке для быстрого восстановления поврежденных данных.

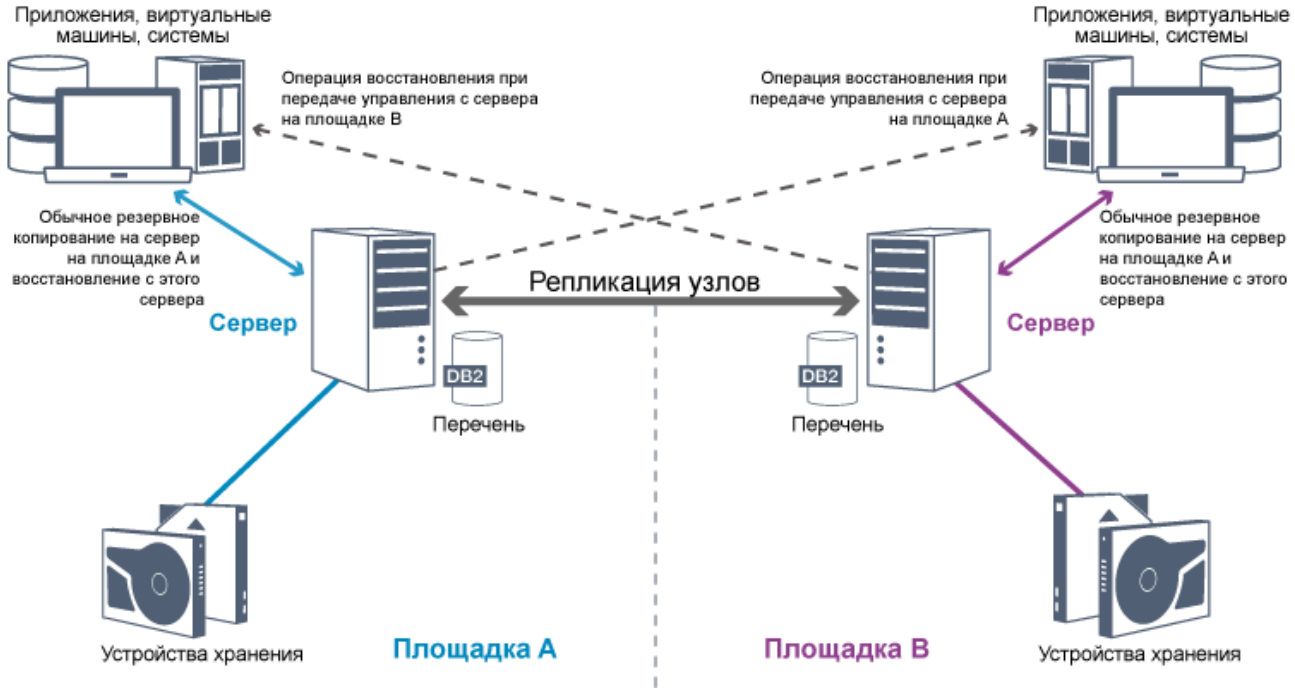
Стратегии для аварийного восстановления с использованием IBM Spectrum Protect

IBM Spectrum Protect обеспечивает несколько путей восстановления сервера, если произойдет отказ базы данных или пулов хранения.

Автоматическая передача управления для аварийного восстановления

Автоматическая передача управления - это операция, которая переключается на резервную систему, если происходит прерывание программы, оборудования или сети. Автоматическая передача управления при отказе используется в сочетании с репликацией узлов для восстановления данных после системного сбоя. На Рис. 1 показан процесс автоматической передачи управления IBM Spectrum Protect при отказе.

Рис. 1. Процесс автоматической передачи управления при отказе



Автоматическая передача управления для восстановления данных происходит в тех случаях, когда исходный сервер репликации недоступен из-за аварии или системного сбоя. При обычных операциях, когда клиент получает доступ к исходному серверу репликации, он получает информацию о соединении с целевым сервером репликации. Клиентский узел хранит информацию о соединении для передачи управления в аварийном случае в клиентском файле опций.

Во время операций восстановления клиента сервер автоматически перенаправляет клиенты с исходного сервера репликации на целевой сервер репликации или наоборот. Для защиты передачи управления при отказе может использоваться только один сервер на один узел. Когда начинается новая операция клиента, он пытается соединиться с исходным сервером репликации. Клиент возобновляет операции на исходном сервере репликации, если этот сервер становится доступен.

Чтобы использовать автоматическую передачу управления для реплицированных клиентских узлов, исходный сервер репликации, сервер репликации назначения и клиент должны быть на уровне версии 7.1 или новее. Если версия любого из серверов более старая, автоматическая передача управления отключается и вам придется положиться на передачу управления при сбое вручную.

Восстановление компонентов IBM Spectrum Protect

База данных сервера, журнал восстановления и пулы хранения имеют ключевое значение для работы IBM Spectrum Protect, и их необходимо защищать. Если база данных непригодна для использования, весь сервер станет недоступным, и восстановление данных, которыми управляет сервер, может оказаться затруднительным или невозможным.

Даже при отсутствии базы данных можно прочитать фрагменты данных или полные файлы с томов хранения, которые у вас не зашифрованы, и это может нарушить безопасность. Поэтому нужно всегда создавать резервную копию базы данных. Кроме того, всегда шифруйте конфиденциальные данные при помощи клиента или устройства хранения, если носитель хранения не защищен физически.

IBM Spectrum Protect обеспечивает несколько методов защиты данных, к которым относятся пулы хранения резервного копирования и база данных. Например, можно задать расписания для выполнения следующих операций.

- После первоначального полного резервного копирования пулов хранения каждую ночь выполняется инкрементное резервное копирование.

- Инкрементное резервное копирование базы данных выполняется каждую ночь.
- Полное резервное копирование базы данных выполняется раз в неделю.

Для сред, основанных на лентах, можно использовать менеджер восстановления после аварий (disaster recovery manager, DRM), которая поможет вам выполнять многие задачи, связанные с защитой и восстановлением данных. DRM поставляется вместе с IBM Spectrum Protect Extended Edition.

Профилактические действия по восстановлению

Для восстановления применяются следующие профилактические действия:

- Зеркальное копирование, за счет которого сервер хранит копию активного журнала
- Резервное копирование базы данных
- Резервное копирование пулов хранения
- Аудит пулов хранения с целью выявления поврежденных файлов и восстановления поврежденных файлов, когда это требуется
- Резервное копирование файлов конфигурации устройств и файлов хронологии томов
- Проверка данных в пулах хранения с использованием циклического контроля по избыточности
- Сохранение файла cert.kdb в надежном месте, чтобы обеспечить безопасность Secure Sockets Layer (SSL)

Если для хранения используется лента, то можно создать план аварийного восстановления, который поможет вам выполнить процесс восстановления с использованием DRM. План аварийного восстановления можно использовать с целью аудита, чтобы подтвердить возможность восстановления сервера. В методах DRM аварийного восстановления применяются следующие действия:

- Создание плана аварийного восстановления для сервера
- Резервное копирование данных сервера на ленту
- Отправка данных резервных копий сервера на удаленную площадку или на другой сервер
- Хранение данных о клиентской системе
- Назначение и отслеживание носителей, используемых для сохранения и восстановления данных клиента

Решения IBM Spectrum Protect для защиты данных

Серверы и клиенты IBM Spectrum Protect обеспечивают решения по защите данных для наиболее распространенных бизнес-требований и требований по соответствию.

- Выбор решения по защите данных для вашей среды
  Чтобы вам было проще внедрить среду защиты данных, прочтите информацию о наиболее успешных на практике конфигурациях IBM Spectrum Protect и выберите лучшее решение в соответствии с вашими бизнес-требованиями.
- Решение с одной площадкой
  Это решение по защите данных обеспечивает экономичное хранение данных на одной площадке при минимальной настройке оборудования.
- Решение с несколькими площадками
  Это решение по защите данных обеспечивает репликацию на нескольких площадках, чтобы каждый сервер защищал данные для другой площадки.
- Ленточное решение
  Это решение для защиты данных обеспечивает хранение на ленточном носителе, это гибкая и экономически доступная возможность долгосрочного хранения данных.
- Документация по решению в файлах PDF
  Вы можете скачать файлы PDF с решениями для защиты данных IBM Spectrum Protect.

Выбор решения по защите данных для вашей среды

Чтобы вам было проще внедрить среду защиты данных, прочтите информацию о наиболее успешных на практике конфигурациях IBM Spectrum Protect и выберите лучшее решение в соответствии с вашими бизнес-требованиями.

- Реализация решения по защите данных на основе дисков для одной площадки
  Эта реализация решения по защите данных на основе дисков для одной площадки с применением IBM Spectrum Protect использует встроенную дедупликацию данных и обеспечивает защиту данных на одной площадке.
- Реализация решения по защите данных на основе дисков для нескольких площадок
  Эта реализация решения по защите данных на основе дисков для одной площадки с применением IBM Spectrum Protect использует встроенную дедупликацию данных и репликацию на двух площадках.

- Реализация решения по защите данных на основе устройств для нескольких площадок
  Эта реализация решения по защите данных IBM Spectrum Protect для нескольких площадок использует дедупликацию данных на основе устройств и репликацию. Резервный сервер конфигурируется на второй площадке, чтобы восстановить данные, если первичный сервер окажется недоступен.
- Реализация решения по защите данных на основе ленты
  Эта реализация решения по защите данных с помощью IBM Spectrum Protect использует одно или несколько устройств хранения на ленте для резервного копирования данных. Резервное копирование на магнитную ленту обеспечивает недорогую масштабируемость, оптимизированную для долгосрочного хранения.
- Сравнение решений по защите данных
  Сравните важнейшие функции всех решений IBM Spectrum Protect, чтобы определить, какая конфигурация лучше всего соответствует вашим требованиям к защите данных. Затем смотрите доступную документацию, чтобы реализовать решение.
- Дорожная карта для реализации решения по защите данных
  Спланируйте и реализуйте наиболее подходящее решение по защите данных для вашей бизнес-среды с использованием IBM Spectrum Protect.

Реализация решения по защите данных на основе дисков для одной площадки

Эта реализация решения по защите данных на основе дисков для одной площадки с применением IBM Spectrum Protect использует встроенную дедупликацию данных и обеспечивает защиту данных на одной площадке.

Это решение по защите данных предоставляет следующие преимущества:

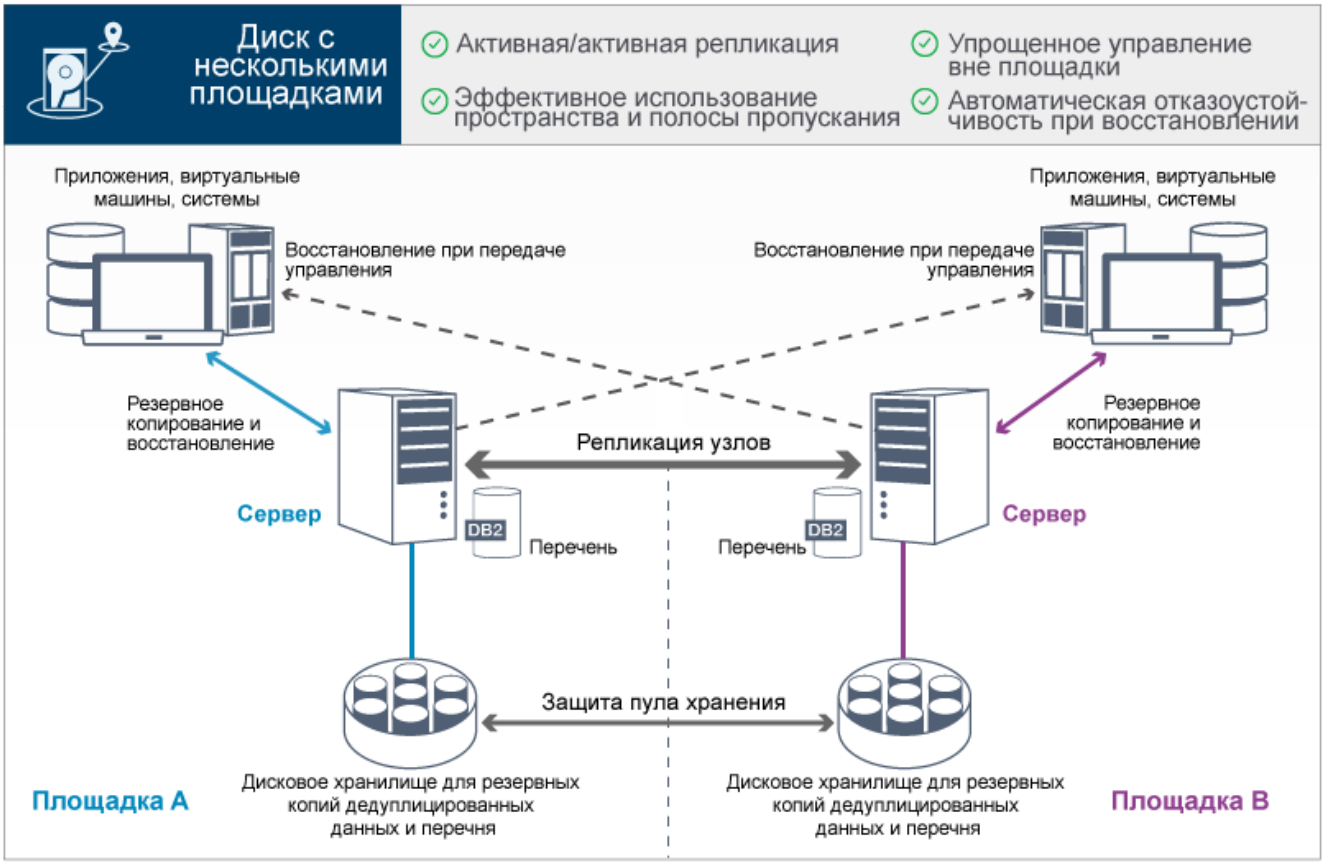
- Оборудование системы сервера и хранения находятся на одной площадке
- Экономичное использование хранения за счет функции дедупликации данных
- Решение с экономичным использованием пространства с минимальной настройкой оборудования
- Минимальная реализация, при которой нужно установить и сконфигурировать только один сервер и поддерживающее его оборудование хранения

В этом решении клиент отправляет данные на сервер IBM Spectrum Protect, где производится дедупликация данных и они сохраняются в пуле хранения каталога-контейнера, реализованном в дисковом пространстве хранения. Для данных из перечня также создается резервная копия в дисковом хранилище. Это решение подходит для сред начального уровня, для которых не требуется вторая копия данных.

Ссылки, связанные с данной:
Сравнение решений по защите данных

Реализация решения по защите данных на основе дисков для нескольких площадок

Эта реализация решения по защите данных на основе дисков для одной площадки с применением IBM Spectrum Protect использует встроенную дедупликацию данных и репликацию на двух площадках.



Это решение по защите данных предоставляет следующие преимущества:

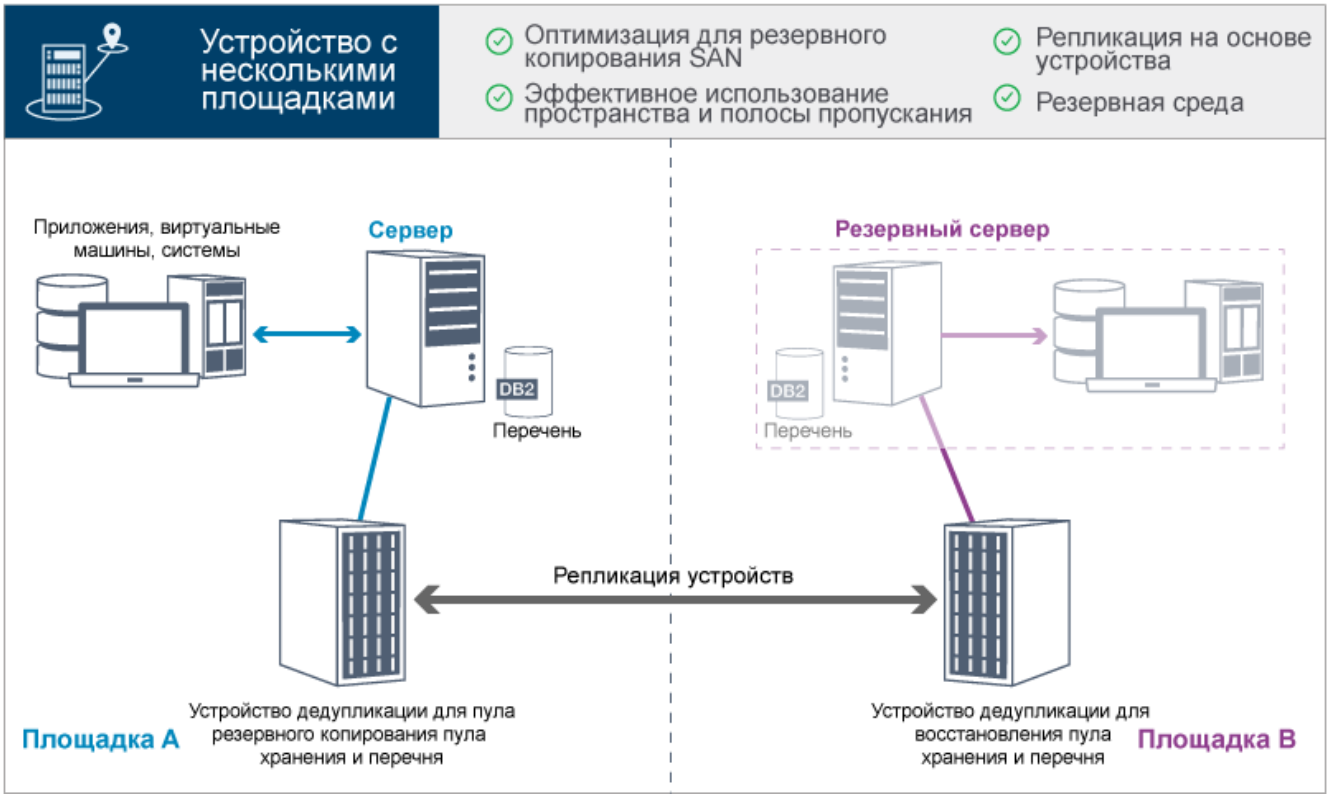
- Репликацию можно сконфигурировать для обеих площадок, чтобы каждый сервер защищал данные для другого сервера
- Упрощено хранение данных вне площадки для каждого расположения
- Полоса пропускания используется эффективно, так как между двумя площадками производится репликация только дедуплицированных данных
- Клиенты могут автоматически перенаправлять работу на сервер назначения репликации, если исходный сервер репликации недоступен

В этом решении клиенты отправляют данные на исходный сервер, где производится дедупликация данных и они сохраняются в пуле хранения каталога-контейнера, реализованном в дисковом пространстве хранения. Данные реплицируются в пуле хранения на целевом сервере для каждой площадки. Это решение подходит для сред, в которых требуется защита от аварий. Если сконфигурирована взаимная репликация, клиенты на обоих площадках могут использовать восстановление при передаче управления для постоянного резервного копирования и восстановления данных с доступного сервера на другой площадке.

Ссылки, связанные с данной:
Сравнение решений по защите данных
Дорожная карта для реализации решения по защите данных

Реализация решения по защите данных на основе устройств для нескольких площадок

Эта реализация решения по защите данных IBM Spectrum Protect для нескольких площадок использует дедупликацию данных на основе устройств и репликацию. Резервный сервер конфигурируется на второй площадке, чтобы восстановить данные, если первичный сервер окажется недоступен.



Это решение по защите данных предоставляет следующие преимущества:

- Производительность оптимизирована для резервного копирования в высокоскоростных сетях хранения данных (storage area network, SAN) и для использования в сочетании с IBM Spectrum Protect для SAN, когда клиенты создают резервные копии непосредственно на виртуальных ленточных устройствах, подключенных к SAN.
- Быстрая репликация на основе устройств освобождает сервер от отслеживания метаданных репликации в базе данных сервера.
- Эффективно используется полоса пропускания и пространство хранения, так как между двумя площадками производится репликация только дедуплицированных данных.
- Резервная среда обеспечивает аварийное восстановление, но не требует того объема ресурсов, который необходим для полностью активного сайта.

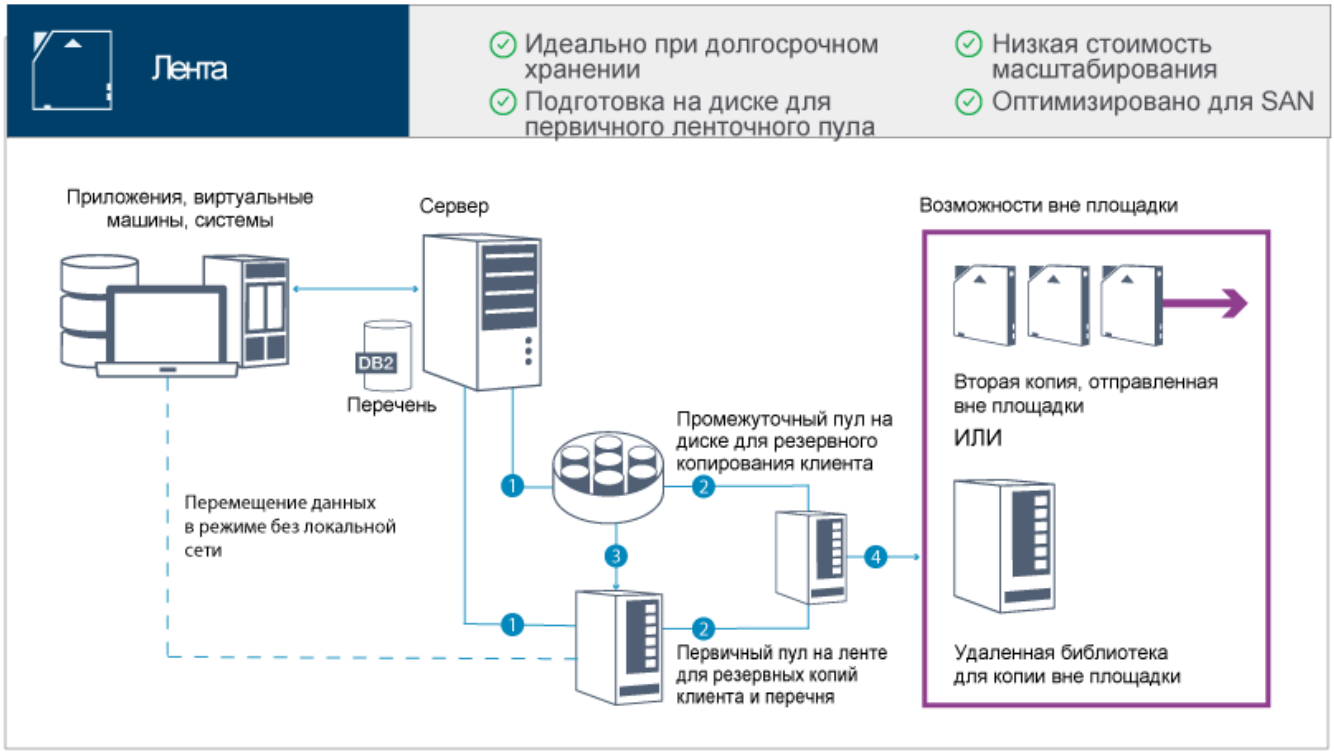
При такой конфигурации защиты данных сервер использует аппаратные устройства для дедупликации и репликации данных. Устройство на площадке A дедуплицирует данные, а затем реплицирует данные на устройство на площадке B для защиты от аварий. Если на площадке A произойдет сбой, вы сделаете резервный сервер активным, восстановив самую последнюю резервную копию базы данных и активировав реплицированную копию данных.

Дополнительную информацию о конфигурировании виртуальных ленточных библиотек смотрите в разделе Конфигурирование виртуальных ленточных библиотек.

Ссылки, связанные с данной:
Сравнение решений по защите данных
Дорожная карта для реализации решения по защите данных

Реализация решения по защите данных на основе ленты

Эта реализация решения по защите данных с помощью IBM Spectrum Protect использует одно или несколько устройств хранения на ленте для резервного копирования данных. Резервное копирование на магнитную ленту обеспечивает недорогую масштабируемость, оптимизированную для долгосрочного хранения.



Это решение по защите данных предоставляет следующие преимущества:

- Производительность оптимизирована для операций резервного копирования в высокоскоростных сетях хранения данных (storage area network, SAN) непосредственно на ленту для типов больших данных и для долгосрочного хранения данных.
- Доступность данных оптимизирована за счет сохранения копий данных вне площадки с тем, чтобы обеспечить возможность восстановления после аварий. Если вы включите функцию управления аварийным восстановлением (disaster recovery management, DRM) и произойдет авария, DRM поможет наладить процесс восстановления ваших серверов.
- Защита данных оптимизирована, так как копии данных хранятся вне площадки на ленточных устройствах, которые *не* соединены с Интернетом. Атаки программ с требованием выкупа основываются на соединении с Интернетом; поэтому хранилище вне площадки может помочь защититься от таких атак.
- Экономичная масштабируемость достигается за счет сокращения потребности в дополнительном дисковом оборудовании и снижения энергетических затрат.

Понятия, связанные с данным:
Выбор драйвера ленточного устройства
Задачи, связанные с данной:
Создание стратегий резервного копирования
Управление перечнем томов
Ссылки, связанные с данной:
Сравнение решений по защите данных
Установка и конфигурирование драйверов ленточных устройств

Сравнение решений по защите данных

Сравните важнейшие функции всех решений IBM Spectrum Protect, чтобы определить, какая конфигурация лучше всего соответствует вашим требованиям к защите данных. Затем смотрите доступную документацию, чтобы реализовать решение.

	Диск с одной площадкой	**Диск с несколькими площадками**	**Устройство с несколькими площадками**	**Лента**
				

	Диск с одной площадкой	**Диск с несколькими площадками**	**Устройство с несколькими площадками**	**Лента**
				
Особенности				
Стоимость	$	$$$	$$$$	$$
Уровень защиты	Одна копия данных	Две или более копии данных	Две или более копии данных	Две или более копии данных
Аварийное восстановление	Нет	Активный сервер	Резервный сервер	Копии вне системы
Важнейшие преимущества				
Качественно новое сокращение объема данных	✓	✓	✓	✓
Быстрые и эффективные операции резервного копирования и восстановления на основе дисков	✓		✓	
Упрощенное управление данными вне системы		✓		
Функция дедупликации данных безо всякой дополнительной оплаты	✓	✓		
Без какой-либо дополнительной оплаты включена обработка репликации		✓		
Дедупликация данных как на исходном, так и на целевом сервере		✓		
Экономичная масштабируемость и оптимизация для долгосрочного хранения				✓
Эффективность и затраты				
Операции резервного копирования, оптимизированные для высокоскоростной сети хранения данных (storage area network, SAN)			✓	✓
Оптимизация для высокоскоростной локальной сети (local area network, LAN)	✓	✓	✓	
Глобальная дедупликация данных для всех типов данных и источников	✓	✓	✓	
Репликация с эффективным использованием полосы пропускания		✓	✓	
Снижение энергетических затрат				✓
Возможность создания второй копии без дополнительных дисковых аппаратных средств				✓
Доступность				
Возможность создания копий вне системы		✓	✓	✓
Репликация на основе устройств			✓	
Восстановление клиента с сервера высокой доступности		✓		
Пункт назначения репликации в облаке		✓		

	Диск с одной площадкой	Диск с несколькими площадками	Устройство с несколькими площадками	Лента
				
Независимое управление политиками хранения для данных репликации; возможность сохранять больше или меньше данных на площадке восстановления		✓		
Репликация на уровне приложений; возможность выбрать, какие системы и приложения реплицируются		✓		
Масштабируемость				
Глобальная дедупликация данных на разных серверах			✓	
Оптимизированное для SAN резервное копирование непосредственно на ленту для типов данных больших объемов				✓
Масштабируемость в петабайтах для одного экземпляра				✓

Что делать дальше

Прочтите доступную документацию для решений в разделе Дорожная карта для реализации решения по защите данных.
Ссылки, связанные с данной:
Реализация решения по защите данных на основе дисков для одной площадки
Реализация решения по защите данных на основе дисков для нескольких площадок
Реализация решения по защите данных на основе устройств для нескольких площадок
Реализация решения по защите данных на основе ленты

Дорожная карта для реализации решения по защите данных

Спланируйте и реализуйте наиболее подходящее решение по защите данных для вашей бизнес-среды с использованием IBM Spectrum Protect.

Решение с одной площадкой

Шаги, в которых описано, как спланировать, реализовать, отслеживать и управлять дисковым решением с одной площадкой, смотрите в разделе Решение с одной площадкой.

Решение с несколькими площадками

Шаги, в которых описано, как спланировать, реализовать, отслеживать и управлять дисковым решением с несколькими площадками, смотрите в разделе Решение с несколькими площадками.

Ленточное решение

Шаги, в которых описано, как спланировать, реализовать, отслеживать и управлять решением с ленточным устройством, смотрите в разделе Ленточное решение.

Решение на основе устройств с несколькими площадками

Обзор задач, которые нужно выполнить, чтобы реализовать решение на основе устройств с несколькими площадками, рассмотрите следующие шаги:

1. Начните планировать решение, ознакомившись с информацией в следующих ссылках:

    - AIX: Планирование емкости
    - Linux: Планирование емкости
    - Windows: Планирование емкости
2. Установите сервер и (необязательно) Центр операций. Ознакомьтесь с информацией по следующим ссылкам:
    - Установка и обновление сервера
    - Установка и обновление Центра операций
3. Сконфигурируйте сервер для хранения данных в виртуальной ленточной библиотеке.
    - Управление виртуальными ленточными библиотеками
    - Подключение ленточных устройств к серверу

   Рекомендации по повышению производительности системы смотрите в разделе Рекомендации по конфигурации.

4. Сконфигурируйте политики для защиты ваших данных. Ознакомьтесь с информацией в разделе Настройка политик.
5. Настройте расписания клиентов. Ознакомьтесь с информацией в разделе Планирование операций резервного копирования и архивирования.
6. Установите и настройте клиенты. Чтобы определить нужный вам тип программы-клиента, смотрите информацию в разделе Добавление клиентов .
7. Настройте мониторинг своей системы. Ознакомьтесь с информацией в разделе Мониторинг решений по хранению.

Ссылки, связанные с данной:
Сравнение решений по защите данных
Реализация решения по защите данных на основе дисков для одной площадки
Реализация решения по защите данных на основе дисков для нескольких площадок
Реализация решения по защите данных на основе устройств для нескольких площадок
Реализация решения по защите данных на основе ленты

Решение с одной площадкой

Это решение по защите данных обеспечивает экономичное хранение данных на одной площадке при минимальной настройке оборудования.

- Планирование дискового решения по защите данных с одной площадкой
  Спланируйте реализацию защиты данных, включающую в себя сервер на одной площадке, где используется дедупликация данных.
- Реализация решения по защите данных для одной площадки
  Дисковое решение для одной площадки конфигурируется на одной площадке и использует дедупликацию данных.
- Мониторинг решения с одной площадкой
  После реализации дискового решения IBM Spectrum Protect с одной площадкой произведите мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.
- Управление операциями для дискового решения с одной площадкой
  Используйте эту информацию для управления операциями при дисковом решении для одной площадки с IBM Spectrum Protect, включающим в себя сервер и использующим дедупликацию данных для одной площадки.

Планирование дискового решения по защите данных с одной площадкой

Спланируйте реализацию защиты данных, включающую в себя сервер на одной площадке, где используется дедупликация данных.

Опции реализации

Сервер можно сконфигурировать для дискового решения с одной площадкой следующими способами:

Конфигурирование сервера с использованием компонента Центр операций и административных команд
В этой документации приводятся шаги по конфигурированию диапазона систем хранения и программы сервера для вашего решения. Задачи по конфигурированию выполняются при помощи мастеров и опций в командах Центр операций и IBM Spectrum Protect. Информацию о том, как начать работу смотрите в разделе Дорожная карта планирования.

Сконфигурируйте сервер при помощи автоматизированных сценариев

Подробные рекомендации по реализации дискового решения с одной площадкой с использованием конкретных систем хранения IBM® Storwize и автоматических сценариев для конфигурирования сервера смотрите в IBM Spectrum Protect Blueprint. Документация и сценарии доступны на сайте IBM developerWorks по адресу: IBM Spectrum Protect Blueprints.

В проектной документации нет шагов по установке и конфигурированию Центр операций или по настройке защищенной связи с использованием Transport Security Layer (TLS). Включена возможность использования Elastic Storage Server на основе технологии IBM Spectrum Scale.

Дорожная карта планирования

Запланируйте дисковое решение с одной площадкой, ознакомившись со схемой архитектуры, показанной ниже на рисунке, а затем выполнив задачи дорожной карты, которые приводятся после диаграммы.

Описанные ниже шаги необходимы, чтобы произвести планирование для дисковой среды с одной площадкой.

1. Выберите размер системы.
2. Выполните требования к аппаратному и программному обеспечению.
3. Запишите значения конфигурации системы в рабочие листы планирования.
4. Спланируйте хранение.
5. Спланируйте защиту.
    a. Спланируйте роли администраторов.
    b. Спланируйте защищенную связь.
    c. Спланируйте хранение шифрованных данных.
    d. Спланируйте доступ через брандмауэр.

Выбор размера системы

Выберите размер сервера IBM Spectrum Protect на основе объема данных, которыми вы управляете, и систем, которые нужно защитить.

Об этой задаче

Информацию в приведенной ниже таблице можно использовать, чтобы определить размер сервера, который вам потребуется, в зависимости от объема данных, которыми вы управляете.

В следующей таблице описан том данных, которым управляет сервер. Этот объем включает в себя все версии. Ежедневный объем данных - это объем данных, резервные копии которых вы создаете ежедневно. И общий объем управляемых данных, и ежедневный объем новых данных измеряются как размер до любого сокращения данных.

Табл. 1. Определение размера сервера

Общий объем управляемых данных	**Ежедневный объем новых данных для резервного копирования**	**Необходимый размер сервера**
60 ТБ - 240 ТБ	До 10 ТБ в день	Малое
196 ТБ - 784 ТБ	10 - 20 ТБ в день	Среднее
1000 ТБ - 4000 ТБ	20 - 100 ТБ в день	Большое

Значения ежедневных резервных копий в таблице основаны на результатах испытаний с объектами по 128 МБ, которые используются компонентом IBM Spectrum Protect for Virtual Environments. Рабочие нагрузки, состоящие из объектов менее 128 КБ, могут не достигать этих ежедневных пределов.

Требования к системе для дискового решения с одной площадкой

После выбора решения IBM Spectrum Protect, наилучшим образом соответствующего вашим требованиям к защите данных, ознакомьтесь с требованиями к системе, чтобы спланировать реализацию решения по защите данных.

Убедитесь, что система соответствует требованиям к аппаратным и программным средствам для сервера того размера, который вы собираетесь использовать.

- Требования к аппаратным средствам
  Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.
- Требования к программному обеспечению
  Документация для дискового решения IBM Spectrum Protect с одной площадкой содержит задачи по установке и конфигурированию для указанных ниже операционных систем. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информация, связанная с данной:
Поддерживаемые операционные системы для IBM Spectrum Protect

Требования к аппаратным средствам

Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.

Определение системных размеров можно найти в t_ssdisk_select_size.html.

В следующей таблице перечислены минимальные требования к аппаратному обеспечению сервера и хранилища на основе размера сервера, который вы собираетесь построить. Если вы используете локальные разделы (LPAR) или рабочие разделы (WPAR), скорректируйте требования к сети, чтобы учесть размер разделов.

В качестве отправной точки используйте информацию, содержащуюся в следующей таблице. Самую свежую информацию о требованиях к оборудованию и спецификациях для сервера и хранилища смотрите в разделе IBM Spectrum Protect Blueprints.

Аппаратный компонент	**Небольшая система**	**Средняя система**	**Крупная система**

Аппаратный компонент	Небольшая система	Средняя система	Крупная система
Процессор сервера	 Операционные системы AIX 6 ядер процессора, 3,42 ГГц или быстрее  Операционные системы Linux  Операционные системы Windows 16 ядер процессора, 1,7 ГГц или быстрее	 Операционные системы AIX 10 ядер процессора, 3,42 ГГц или быстрее  Операционные системы Linux  Операционные системы Windows 20 ядер процессора, 2,2 ГГц или быстрее	 Операционные системы AIX 20 ядер процессора, 3,42 ГГц  Операционные системы Linux  Операционные системы Windows 44 ядра процессора, 2,2 ГГц или быстрее
Память сервера	64 ГБ ОП	128 ГБ ОП	256 ГБ ОП
Сеть	• 10 ГБ Ethernet (1 порт) • Адаптер 8 ГБ Fibre Channel (2 порта)	• 10 ГБ Ethernet (2 порта) • Адаптер 8 ГБ Fibre Channel (2 порта)	• 10 ГБ Ethernet (4 порта) • Адаптер 8 ГБ Fibre Channel (4 порта)
Хранение	• Диски SSD 1,45 Тб для базы данных, плюс пространство для записей Центр операций • 67 ТБ пула хранения каталогов-контейнеров с дедупликацией	• Диски SSD 2,53 Тб для базы данных, плюс пространство для записей Центр операций • 207,9 ТБ пула хранения каталогов-контейнеров с дедупликацией	• Диски SSD 6,54 Тб для базы данных, плюс пространство для записей Центр операций • 1049,67 ТБ пула хранения каталогов-контейнеров с дедупликацией

Оценка необходимого объема пространства для базы данных Центр операций

Требования к аппаратным средствам для Центр операций включены в предыдущую таблицу за исключением пространства базы данных и архивного журнала (перечня), которые используются компонентом Центр операций для удерживания записей для управляемых клиентов.

Если вы не собираетесь устанавливать Центр операций на том же компьютере, что и сервер, вы можете оценить требования к системе отдельно. Чтобы вычислить требования к системе для компонента Центр операций, смотрите описание калькулятора требований к системе в документе техническое замечание 1641684.

Управление компонентом Центр операций на сервере - это рабочая нагрузка, требующая дополнительного пространства для операций базы данных. Объем пространства зависит от числа клиентов, мониторинг которых осуществляется на сервере. Прочтите следующие рекомендации, которые позволяют оценить, какой объем пространства потребуется вашему серверу.

Пространство базы данных

Компонент Центр операций использует, примерно, 1,2 ГБ пространства базы данных на каждую 1000 клиентов, отслеживаемых на сервере. Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1500 клиентов. Эта конфигурация дает в итоге 6500 клиентов на четырех серверах, и для нее требуется примерно 8,4 ГБ пространства базы данных. Это значение вычисляется путем округления 6500 клиентов до следующей ближайшей 1000, что составит 7000:

```
7 x 1,2 ГБ=8,4 ГБ
```

Пространство архивного журнала

Центр операций использует, примерно, 8 ГБ пространства архивного журнала каждые 24 часа для каждой 1000 клиентов. В примере 6500 клиентов работают через хаб-серверы и подчиненные сервера, и за 24 часа для хаб-сервера используется 56 ГБ пространства архивного журнала.

Для каждого подчиненного сервера в примере пространство архивного журнала, используемое в течение 24 часов, составит около 16 ГБ. Эти оценки основаны на интервале сбора данных о состоянии по умолчанию, равном 5 минутам. Если вы сократите интервал сбора данных с одного раза за 5 минут до одного раза за 3 минуты,

требования к пространству возрастут. В следующих примерах показано примерное увеличение требований к пространству журнала при интервале сбора данных один раз в 3 минуты:

- Хаб-сервер: С 56 ГБ примерно до 94 ГБ
- Каждый подчиненный сервер: С 16 ГБ примерно до 28 ГБ

Увеличьте пространство архивного журнала так, чтобы у вас было достаточно доступного пространства для поддержки компонента Центр операций и чтобы это не влияло на существующие операции сервера.

Требования к программному обеспечению

Документация для дискового решения IBM Spectrum Protect с одной площадкой содержит задачи по установке и конфигурированию для указанных ниже операционных систем. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информацию о требованиях к программам для драйверов устройств IBM® lin_tape смотрите в разделе Руководство по установке и использованию IBM Tape Device Drivers.

Системы AIX

Тип ПО	**Минимальные требования к программному обеспечению**
Операционная система	IBM AIX 7.1 Дополнительную информацию о требованиях к операционным системам смотрите в разделе AIX: инимальные требования к системе для систем AIX.
Утилита gunzip	Утилита gunzip должна быть доступна в вашей системе до установки или обновления сервера IBM Spectrum Protect. Убедитесь, что утилита gunzip установлена и ее путь задан в переменной среды PATH.
Тип файловой системы	Файловые системы JFS2 Системы AIX могут кэшировать большие объемы данных файловой системы; при этом может сокращаться объем памяти, необходимый серверу и процессам IBM DB2. Чтобы избежать подкачки при использовании сервера AIX, используйте для файловой системы JFS2 опцию монтирования rbrw. Для кэша файловой системы используется меньше памяти, и для IBM Spectrum Protect будет доступно больше памяти. Не используйте опции монтирования файловой системы с параллельным вводом-выводом (Concurrent I/O, CIO) и с прямым вводом-выводом (Direct I/O, DIO) для файловых систем, содержащих журналы базы данных IBM Spectrum Protect или тома пулов хранения. Использование этих опций может вызывать снижение производительности многих серверных операций. IBM Spectrum Protect и DB2 все равно могут использовать DIO там, где это выгодно, но для IBM Spectrum Protect не требуются опции монтирования, чтобы выборочно использовать преимущества этого метода.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Linux

Тип ПО	**Минимальные требования к программному обеспечению**
Операционная система	Red Hat Enterprise Linux 7 (x86_64)
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, устанавливаемые в системе IBM Spectrum Protect. Серверы Red Hat Enterprise Linux: • libaio • libstdc++.so.6 (требуются 32- и 64-разрядные пакеты) • numactl.x86_64

Тип ПО	Минимальные требования к программному обеспечению
Тип файловой системы	Сформатируйте файловые системы, связанные с базами данных, используя ext3 или ext4. Для файловых систем, связанных с пулами, используйте XFS.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Windows

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Microsoft Windows Server 2012 R2 (64-разрадная система) или Windows Server 2016
Тип файловой системы	NTFS
Другое программное обеспечение	Должны быть установлены и включены Windows 2012 R2 или Windows 2016 с платформой .NET Framework 3.5. Должны быть отключены следующие политики управления учетными записями пользователей: • Управление учетными записями пользователей: Режим Утверждать администраторов для встроенной учетной записи Администратор • Управление учетными записями пользователей: Запускать всех администраторов в режиме Утверждать администраторов

Задачи, связанные с данной:

Настройка сетевых опций AIX

Рабочие листы планирования

Используйте рабочие таблицы планирования, чтобы записывать в них значения, которые вы используете при настройке системы с последующим конфигурированием сервера IBM Spectrum Protect. Используйте наилучшие практические значения по умолчанию, приведенные в рабочих таблицах.

Каждая рабочая таблица поможет вам подготовиться к разным стадиям конфигурирования системы за счет использования наилучших практических значений:

Предварительное конфигурирование серверной системы
: Используйте рабочие таблицы предварительного конфигурирования для планирования файловых систем и каталогов, которые вы создадите, когда сконфигурируете файловые системы для IBM Spectrum Protect во время настройки системы. Все каталоги, созданные вами для сервера, должны быть пустыми.

Конфигурация сервера
: Воспользуйтесь рабочими таблицами по конфигурированию, когда будете конфигурировать сервер. Для большинства элементов предлагаются значения по умолчанию, кроме случаев, когда это отмечено.

AIX

Табл. 1. Рабочая таблица для предварительного конфигурирования серверной системы AIX

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	/home/tsminst1/tsminst1		50 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 2.
Каталог для установки сервера	/		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/usr		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/var		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/tmp		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/opt		Доступное пространство, необходимое для каталога: 10 ГБ	
Каталог для активного журнала	/tsminst1/TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	Если вы создаете активный журнал при первоначальном конфигурировании сервера, задайте размер, равный 128 ГБ.
Каталог для архивного журнала	/tsminst1/TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для базы данных	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем
Каталоги для хранения	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 2. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 1, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	passw0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра DB2	tsmsrvrs		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Linux

Табл. 3. Рабочая таблица для предварительного конфигурирования серверной системы Linux

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	/home/tsminst1/tsminst1		25 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 4.
Каталог для активного журнала	/tsminst1/TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	
Каталог для архивного журнала	/tsminst1/TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	
Каталоги для базы данных	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для хранения	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 4. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 3, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	passw0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра DB2	tsmsrvrs		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Windows

Поскольку много томов создается для сервера, сконфигурируйте сервер, используя имеющуюся в Windows функцию отображения дисковых томов в каталоги, а не в буквы дисков.

Например, C:\tsminst1\TSMdbpsace00 - это точка монтирования для тома с его собственным пространством. Том отображается в каталог на диске C:, но не занимает пространство на диске C:. Исключением является каталог экземпляра сервера, C:\tsminst1, который может быть точкой монтирования или обычным каталогом.

Табл. 5. Рабочая таблица для предварительного конфигурирования серверной системы Windows

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	C:\tsminst1		25 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 6.
Каталог для активного журнала	C:\tsminst1\TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	
Каталог для архивного журнала	C:\tsminst1\TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	
Каталоги для базы данных	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для хранения	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 6. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 5, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	pAssW0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Планирование хранения

Выберите наиболее эффективную технологию хранения для компонентов IBM Spectrum Protect, чтобы обеспечить эффективную работу сервера и высокую производительность операций.

У аппаратных устройств хранения разные характеристики емкости и производительности, что определяет то, как их можно эффективно использовать вместе с IBM Spectrum Protect. Общие рекомендации по выбору соответствующего оборудования хранения и настройке вашего решения смотрите в указанных ниже источниках.

База данных и активный журнал

- Используйте для базы данных и активного журнала IBM Spectrum Protect быстрый диск, например, со следующими характеристиками:
  - Высокопроизводительный диск 15 K rpm с оптоволоконным (Fibre Channel) или последовательно подключенным интерфейсом SCSI (SAS).
  - Твердотельный диск (Solid-state disk, SSD)

- Изолируйте активный журнал от базы данных, если вы не используете твердотельное (SSD) или флеш-оборудование
- При создании массивов для базы данных используйте RAID уровня 5

Пул хранения

- Для пула хранения можно использовать менее дорогие и более медленные диски
- Пул хранения данных может совместно использовать диски для хранения архивного журнала и резервной копии базы данных
- Используйте RAID уровня 6 для массивов пулов хранения, чтобы добавить защиту от двойных сбоев диска при использовании крупных типов дисков

- Планирование массивов хранения
  Подготовьтесь к конфигурированию дискового хранения, спланировав массивы RAID и тома в соответствии с размером вашей системы IBM Spectrum Protect.

Ссылки, связанные с данной:
Требования к системе хранения и уменьшение риска повреждения данных

Планирование защиты

Спланируйте защиту систем в решении IBM Spectrum Protect, используя управление доступом и аутентификацией, и рассмотрите возможность шифрования данных и передачи паролей.

Рекомендации относительно защиты вашей среды хранения от атак программ, требующих выкуп, и восстановления среды хранения, если произойдет атака, смотрите в разделе Защита среды хранения против программ-вымогателей.

- Планирование ролей администратора
  Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.
- Планирование защищенной связи
  План защиты взаимодействий между компонентами решения IBM Spectrum Protect.
- Планирование хранения зашифрованных данных
  Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите возможности, которые лучше всего подходят для ваших требований.
- Планирование доступа через брандмауэр
  Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

Планирование ролей администратора

Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.

Администраторам можно назначить один из следующих уровней полномочий:

Система
: У администраторов с системными полномочиями - высший уровень полномочий. Администраторы с этим уровнем полномочий могут выполнить любую задачу. Они могут управлять всеми доменами политики и пулами хранения и предоставлять полномочия другим администраторам.

Политика
: Администраторы, у которых есть полномочия политики, могут управлять всеми задачами, связанными с управлением политикой. Эти полномочия могут быть неограниченными или могут быть ограничены определенными доменами политики.

Хранение
: Администраторы, у которых есть полномочия хранения, могут выделить ресурсы хранения для сервера и управлять ими.

Оператор
: Администраторы, у которых есть полномочия оператора, могут управлять непосредственной работой сервера и доступностью таких носителей хранения, как ленточные библиотеки и накопители.

В сценариях в Табл. 1 представлены примеры того, почему вам может потребоваться назначить разные уровни полномочий, чтобы администраторы могли выполнять задачи:

Табл. 1. Сценарии для ролей администраторов

Сценарий	Тип ID администратора, который нужно задать
Администратор в небольшой компании управляет сервером и отвечает за все операции сервера.	• Системные полномочия: 1 ID администратора
Администратор нескольких серверов также управляет всей системой. Несколько других администраторов управляют своими собственными пулами хранения.	• Системные полномочия на всех серверах: 1 ID администратора для всех задач по администрированию системы • Полномочия на хранение для назначенных пулов хранения: 1 ID администратора для каждого из других администраторов
Администратор управляет двумя серверами. Другой сотрудник помогает выполнять задачи по администрированию. Два помощника отвечают за то, чтобы производилось резервное копирование важных систем. Каждый помощник отвечает за мониторинг запланированных операций по резервному копированию на одном из серверов IBM Spectrum Protect.	• Системные полномочия на обоих серверах: 2 ID администратора • Полномочия оператора: 2 ID администраторов для помощников с доступом к серверу, за который отвечает каждый сотрудник

Планирование защищенной связи

План защиты взаимодействий между компонентами решения IBM Spectrum Protect.

Определите уровень защиты, требующийся для ваших данных, на основе нормативов и бизнес-требований, которые действуют в вашей компании.

Если для вашего бизнеса требуется высокий уровень защиты паролей и передаваемых данных, запланируйте реализацию защищенной связи на основе протоколов Transport Layer Security (TLS) или Secure Sockets Layer (SSL).

TLS и SSL обеспечивают защищенную связь между сервером и клиентом, но могут отрицательно влиять на производительность системы. Чтобы повысить производительность системы, используйте TLS для аутентификации без шифрования данных объектов. Чтобы указать, использует ли сервер TLS 1.2 для всего сеанса или только для аутентификации, смотрите описание опции клиента SSL для взаимодействий клиента с сервером и параметра UPDATE SERVER=SSL для взаимодействий сервера с сервером. Beginning in V8.1.2, TLS is used for authentication by default. Если вы решите использовать TLS для шифрования всего сеанса, используйте этот протокол только для сеансов, в которых это необходимо, и добавьте на сервер процессорные ресурсы, чтобы справиться с увеличением сетевого трафика. Также можно попробовать использовать другие опции. Например, в некоторых сетевых устройствах, например, в маршрутизаторах и коммутаторах, есть функция TLS или SSL.

TLS и SSL можно использовать для защиты некоторых или всех различных возможных путей связи, например:

- Центр операций: браузер с хабом; хаб с подчиненным сервером
- Клиент с сервером
- Сервер с сервером: репликация узлов

Задачи, связанные с данной:
Защита связи

Планирование хранения зашифрованных данных

Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите возможности, которые лучше всего подходят для ваших требований.

Если вашей компания требуется шифровать данные в пулах хранения, вы можете использовать шифрование IBM Spectrum Protect или такое внешнее устройство, как лента для шифрования.

Если вы выбираете IBM Spectrum Protect для шифрования данных, на клиенте потребуются дополнительные вычислительные ресурсы, что может повлиять на производительность процессов резервного копирования и восстановления.

Информация, связанная с данной:
technote 1963635

Планирование доступа через брандмауэр

Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

В разделе Табл. 1 описаны порты, используемые сервером, клиентом и компонентом Центр операций.

Табл. 1. Порты, используемые сервером, клиентом и компонентом Центр операций

Элемент	**По умолчанию**	**Направление**	**Описание**
Базовый порт (TCPPORT)	1500	Исходящие/ входящие	Для каждого экземпляра сервера требуется уникальный порт. Вместо порта по умолчанию можно задать альтернативный номер порта. Опция TCPPORT принимает от клиента как сеансы TCP/IP, так и сеансы с поддержкой SSL. Для трафика клиента администрирования можно задать значения портов, используя опции TCPADMINPORT и ADMINONCLIENTPORT.
SSL-only port (SSLTCPPORT)	Значения по умолчанию нет	Исходящие/ входящие	Этот порт используется, если вы хотите ограничить взаимодействия на порту только сеансами, поддерживающими SSL. Чтобы обеспечить поддержку взаимодействий как SSL, так и не SSL, используйте опции TCPPORT или TCPADMINPORT.
SMB	45	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SSH	22	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SMTP	25	Исходящие	Этот порт используется для отправки оповещений с сервера по электронной почте.
NDMP	Значения по умолчанию нет	Входящие/ исходящие	Сервер должен иметь возможность открыть соединение исходящего управляющего порта NDMP с устройством NAS. Исходящий управляющий порт - это низкоуровневый адрес в определении функции перемещения данных для устройства NAS. При восстановлении с файл-сервера NDMP на сервер сервер должен иметь возможность открыть соединение исходящего соединения данных NDMP с устройством NAS. Порт соединения данных, который используется при восстановлении, можно сконфигурировать на устройстве NAS. При создании резервных копий с файл-сервера NDMP на сервер устройство NAS должно иметь возможность открыть исходящие соединения данных с сервером, а сервер должен быть способен принять входящие соединения данных NDMP. При помощи серверной опции NDMPPORTRANGE можно ограничить набор портов, доступных для использования в качестве соединений данных NDMP. Вы можете сконфигурировать брандмауэр для соединения с этими портами.
Репликация	Значения по умолчанию нет	Исходящие/ входящие	Порт и протокол для исходящего порта при репликации заданы командой DEFINE SERVER, которая используется, чтобы настроить репликацию. Входящие порты для репликации - это порты TCP и порты SSL, которые исходный сервер указывает в команде DEFINE SERVER.

Элемент	По умолчанию	Направление	Описание
Порт клиентских расписаний	Порт клиента: 1501	Исходящие	Клиент осуществляет прием на указанном порту и передает номер порта серверу. Сервер соединяется с клиентом, если используется планирование по приглашению сервера. Можно задать альтернативный номер порта в файле опций клиента.
Длительно выполн. сеансы	Параметр KEEPALIVE: YES	Исходящие	Если включена опция KEEPALIVE, пакеты проверки активности (keepalive) отправляются во время сеансов клиент-сервер, чтобы не дать программе брандмауэра закрыть длительно выполняющиеся, неактивные соединения.
Центр операций	HTTPS: 11090	Входящие	Эти порты используются для веб-браузера компонента Центр операций. Можно задать альтернативный номер порта.
Порт службы управления клиентами	Порт клиента: 9028	Входящие	Порт службы управления клиентами должен быть доступен из компонента Центр операций. Убедитесь, что брандмауэры не запрещают соединения. Служба управления клиентами использует порт TCP сервера клиентского узла для аутентификации, используя административный сеанс.

Реализация решения по защите данных для одной площадки

Дисковое решение для одной площадки конфигурируется на одной площадке и использует дедупликацию данных.

Путеводитель по реализации

Описанные ниже шаги необходимы, чтобы настроить дисковую среду IBM Spectrum Protect с одной площадкой.

1. Настройте систему.
    a. Сконфигурируйте аппаратуру хранилища и настройте массивы хранения, соответствующие размеру вашей среды.
    b. Установите операционную систему сервера.
    c. Сконфигурируйте ввод-вывод с несколькими путями.
    d. Создайте ID пользователя для экземпляра сервера.
    e. Подготовьте файловые системы для IBM Spectrum Protect.
2. Установите сервер и Центр операций.
3. Сконфигурируйте сервер и Центр операций.
    a. Выполните первоначальное конфигурирование сервера.
    b. Задайте опции сервера.
    c. Сконфигурируйте SSL (Secure Sockets Layer) для сервера и клиента.
    d. Сконфигурируйте Центр операций.
    e. Зарегистрируйте свою лицензию на IBM Spectrum Protect.
    f. Настройте дедупликацию данных.
    g. Задайте правила хранения данных для вашего бизнеса.
    h. Задайте расписания обслуживания сервера.
    i. Задайте расписания клиентов.
4. Установите и сконфигурируйте клиенты.
    a. Зарегистрируйте клиенты и назначьте их для расписаний.
    b. Установите и проверьте службу управления клиентом.
    c. Сконфигурируйте Центр операций на использование службы управления клиентом.
5. Завершите реализацию.

Настройка системы

Чтобы настроить систему, нужно сначала сконфигурировать дисковое оборудование хранения и серверную систему для IBM Spectrum Protect.

- Конфигурирование оборудования систем хранения
  Чтобы сконфигурировать оборудование систем хранения, прочтите общие рекомендации по дисковым системам и IBM Spectrum Protect.

- Установка операционной системы сервера
  Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.
- Конфигурирование ввода-вывода с несколькими путями
  Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.
- Создание ID пользователя для сервера
  Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.
- Подготовка файловых систем для сервера
  Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

Конфигурирование оборудования систем хранения

Чтобы сконфигурировать оборудование систем хранения, прочтите общие рекомендации по дисковым системам и IBM Spectrum Protect.

Процедура

1. Задайте соединение между сервером и устройствами хранения, следуя приведенным ниже рекомендациям:
   - Используйте коммутируемое или прямое усоединение для соединений Fibre Channel.
   - Подберите число портов для соединения и учетную запись для необходимой ширины полосы пропускания.
   - Подберите число портов для соединения на сервере и число портов хоста в дисковой системе.
2. Убедитесь, что драйверы устройств и встроенная микропрограмма в системе сервера, адаптеров и операционной системы, являются современными и находятся на рекомендуемых уровнях.
3. Сконфигурируйте массивы хранения. Убедитесь, что вы правильно произвели планирование, чтобы обеспечить оптимальную производительность. Дополнительную информацию смотрите в разделе Планирование хранения.
4. Убедитесь, что у системы сервера есть доступ к созданным дисковым томам. Сделайте следующее:
   a. Если система подключена к коммутатору Fibre Channel, произведите зонирование сервера, чтобы увидеть диски.
   b. Отобразите все тома, чтобы сообщить дисковой системе, что данному серверу разрешено видеть каждый диск.

Установка операционной системы сервера

Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.

- Установка в системах AIX
  Выполните следующие действия, чтобы установить AIX в системе сервера.
- Установка в системах Linux
  Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.
- Установка в системах Windows
  Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Установка в системах AIX

Выполните следующие действия, чтобы установить AIX в системе сервера.

Процедура

1. Установите AIX версии 7.1 TL4, SP2 или новее в соответствии с инструкциями производителя.
2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

```
127.0.0.1 localhost
```

4. Включите полты выполнения ввода-вывода AIX, введя следующую команду:

   ```
   chdev -l iocp0 -P
   ```

   На производительность сервера может влиять определение часового пояса по Олсону (Olson).
5. Чтобы оптимизировать производительность, измените формат часового пояса с Olson на POSIX. Чтобы обновить параметр часового пояса, используйте следующий формат команды:

   ```
   chtz=локальный_часовой_пояс,дата/время,дата/время
   ```

   Например, если вы находитесь в Тьюсоне (Аризона), где используется стандартное горное время, то вы бы, чтобы перейти к формату POSIX, ввели бы следующую команду:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Добавьте запись в файл .profile пользователя экземпляра, чтобы была задана следующая среда:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Совет: Если пользователь экземпляра недоступен, то выполните этот шаг позже, когда пользователь экземпляра станет доступен.
7. Настройте систему на создание полных файлов ядра приложения. Введите следующую команду:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Чтобы обеспечить взаимодействия с сервером и компонентом Центр операций, убедитесь, что на всех брандмауэрах, которые могут существовать, открыты следующие порты:
   - Для связи с сервером откройте порт 1500.
   - Чтобы обеспечить защищенную связь с компонентом Центр операций, откройте порт 11090 на хаб-сервере.

   Если вы не используете значения портов по умолчанию, то убедитесь, что используемые вами порты открыты.

9. Включите усовершенствования высокой производительности TCP. Введите следующую команду:

   ```
   no -p -o rfc1323=1
   ```

10. Чтобы обеспечить оптимальную пропускную способность и надежность, свяжите вместе четыре порта 10 Gb Ethernet. Используйте инструмент System Management Interface Tool (SMIT), чтобы связать порты друг с другом, используя Etherchannel. При тестировании использовались следующие параметры:

    ```
    режим            8023ad
    auto_recovery    yes            Включить автоматическое восстановление после
                                    передачи управления
    backup_adapter   NONE           Адаптер, используемый при ошибке всего канала
    hash_mode        src_dst_port   Указывает, как выбирается исходящий адаптер
    interval         long           Определяет значение интервала для режима
                                    IEEE 802.3ad
    mode             8023ad         Режим EtherChannel для операции
    netaddr          0              Адрес для команды ping
    noloss_failover  yes            Включает передачу управления без потери данных
                                    после неудачного завершения ping
    num_retries      3              Сколько раз повторять ping, прежде чем заключить
                                    о неудаче
    retry_time       1              Время ожидания (в сек.) между командами ping
    use_alt_addr     no             Включить другой адрес EtherChannel
    use_jumbo_frame  no             Включить фреймы Gigabit Ethernet Jumbo
    ```

11. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 1. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 1. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	**Установка**	**Значение**	**Команда для запроса значения**
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Linux

Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.

Прежде чем начать

Операционная система устанавливается на внутренних жестких дисках. Сконфигурируйте внутренние жесткие диски, используя аппаратный массив RAID 1. Например, если вы конфигурируете небольшую систему, два внутренних диска по 300 ГБ зеркально отражаются в RAID 1, в результате чего для программы установки операционной системы будет доступен один диск в 300 ГБ.

Процедура

1. Установите Red Hat Enterprise Linux версии 7.1 или новее в соответствии с инструкциями производителя. Получите загрузочный DVD-диск, содержащий Red Hat Enterprise Linux версии 7.1 и запустите свою систему с этого DVD-диска. Опции установки смотрите в приведенных ниже рекомендациях. Если элемент не упомянут в приведенном ниже списке, оставьте для него значение по умолчанию.
   a. После запуска DVD-диска выберите в меню Установить или обновить существующую систему.
   b. В окне с приветствием выберите Проверить этот носитель и установить Red Hat Enterprise Linux 7.1.
   c. Выберите предпочтения языка и клавиатуры.
   d. Выберите свое расположение, чтобы задать нужный часовой пояс.
   e. Выберите Выбор программ, а затем в следующем окне выберите Сервер с графическим пользовательским интерфейсом.
   f. На странице сводной информации установки щелкните по Пункт назначения установки и проверьте следующее:
      - В качестве пункта назначения установки выбирается локальный диск на 300 ГБ.
      - В разделе Другие опции хранения выбирается опция Автоматически сконфигурировать разбиение на разделы.

      Щелкните по Готово.
   g. Щелкните по Начать установку . После запуска установки задайте пароль пользователя root для учетной записи пользователя root.

   По завершении установки перезапустите систему и войдите в систему от имени пользователя root. Введите команду df, чтобы проверить базовое разбиение на разделы. Например, в тест-системе первоначальные разделы выдали следующий результат:

```
[root@tvapp02]# df -h
Файловая сист.                Размер Исп. Дост. Исп. % Где смонтир.
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G    1%    /dev/shm
tmpfs                   32G   8.8M  32G    1%    /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
```

```
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
   Чтобы обеспечить оптимальную пропускную способность и надежность, рассмотрите возможность связать вместе несколько сетевых портов. Это можно выполнить, создав сетевое соединение Link Aggregation Control Protocol (LACP), которое агрегирует несколько подчиненных портов в одно логическое соединение. Предпочтительный метод состоит в том, чтобы использовать режим связи 802.3ad, параметр miimon, равный 100, и параметр xmit_hash_policy, равный layer3+4.
   Ограничение: Для использования сетевого соединения LACP у вас должен быть сетевой коммутатор, поддерживающий LACP.

   Дополнительные инструкции по конфигурированию привязанных сетевых соединения при использовании Red Hat Enterprise Linux версии 7 смотрите в документе: Создать интерфейс привязки каналов.

3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

     ```
     127.0.0.1 localhost
     ```

4. Установите компоненты, необходимые для установки сервера. Выполните описанные ниже шаги, чтобы создать репозиторий Yellowdog Updater Modified (YUM) и установить необходимые пакеты.
   a. Смонтируйте DVD-диск установки Red Hat Enterprise Linux в системном каталоге. Например, чтобы смонтировать его в каталоге /mnt, введите следующую команду:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Убедитесь, что DVD-диск смонтирован, введя команду mount. Должна появиться выходная информация, аналогичная следующему примеру:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Перейдите в каталог репозитория YUM, введя следующую команду:

      ```
      cd /etc/yum/repos.d
      ```

      Если каталог repos.d не существует, создайте его.
   d. Вызовите список содержимого каталога:

      ```
      ls rhel-source.repo
      ```

   e. Переименуйте исходный файл repo, введя команду mv. Например:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Создайте новый файл repo, используя текстовый редактор. Например, чтобы использовать редактор vi, введите следующую команду:

      ```
      vi rhel71_dvd.repo
      ```

   g. Добавьте в новый файл repo следующие строки. Параметр baseurl задает точку монтирования каталога:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h. Установите необходимый пакет ksh.x86_64, введя команду yum. Например:

      ```
      yum install ksh.x86_64
      ```

      Исключительная ситуация: Устанавливать библиотеки compat-libstdc++-33-3.2.3-69.el6.i686 и libstdc++.i686 для Red Hat Enterprise Linux версии 7.1 не нужно.
5. По завершении установки программы вы сможете восстановить исходные значения репозитория YUM, выполнив следующие шаги:

a. Размонтируйте DVD-диск установки Red Hat Enterprise Linux, введя следующую команду:

```
unmount /mnt
```

b. Перейдите в каталог репозитория YUM, введя следующую команду:

```
cd /etc/yum/repos.d
```

c. Переименуйте созданный вами файл repo:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Переименуйте исходный файл, используя его исходное имя:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Определите, требуется ли измерения параметров ядра. Сделайте следующее:
   a. Используйте команду sysctl -a, чтобы вывести список значений параметров.
   b. Проанализируйте результаты, следуя рекомендациям в разделе Табл. 1, чтобы определить, не требуются ли какие-либо изменения.
   c. Если требуются изменения, задайте параметры в файле /etc/sysctl.conf. Изменения файлов применяются при запуске системы.

Совет: Автоматически корректируйте значения параметров ядра и устраните необходимость обновления этих параметров вручную. В Linux продукт программное обеспечение баз данных DB2 автоматически корректирует значения параметров ядра взаимодействий между процессами (interprocess communication, IPC) до предпочтительных значений. Чтобы получить дополнительную информацию о значениях параметров ядра, ищите параметры ядра Linux в публикации Документация по продукту DB2 версии 11.1 IBM.

Табл. 1. Оптимальные значения параметра ядра Linux

Параметр	**Описание**
kernel.shmmni	Максимальное число сегментов.
kernel.shmmax	Максимальный размер сегмента совместно используемой памяти (в байтах). Этот параметр нужно задать до автоматического запуска сервера IBM Spectrum Protect при запуске системы.
kernel.shmall	Максимальное число размещенных страниц совместно используемой памяти.
kernel.sem Существует четыре значения для параметра kernel.sem.	(SEMMSL) Максимальное число семафоров на массив.
	(SEMMNS) Максимальное число семафоров на систему.
	(SEMOPM) Максимальное число операций на вызов семафора.
	(SEMMNI) Максимальное число массивов.
kernel.msgmni	Максимальное число очередей сообщений уровня системы.
kernel.msgmax	Максимальный размер сообщения (в байтах).
kernel.msgmnb	Максимальный размер очереди по умолчанию (в байтах).
kernel.randomize_va_space	Параметр kernel.randomize_va_space конфигурирует использование памяти ASLR для ядра. Отключите ASLR, так как это может вызвать ошибки в программе DB2. Дополнительные подробности об ASLR Linux и DB2 смотрите в документе техническое замечание 1365583.

Параметр	Описание
vm.swappiness	Параметр vm.swappiness определяет, может ли ядро выполнять своппинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.
vm.overcommit_memory	Параметр vm.overcommit_memory влияет на то, какой объем виртуальной памяти ядро разрешает выделить. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.

7. Откройте порты брандмауэра для взаимодействия с сервером. Сделайте следующее:
   a. Определите зону, используемую сетевым интерфейсом. По умолчанию, это общедоступная зона.
      Введите следующую команду:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Чтобы использовать адрес порта по умолчанию для взаимодействия с сервером, откройте порт TCP/IP 1500 на брандмауэре Linux.
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Если вы хотите использовать какое-либо значение, отличающееся от значения по умолчанию, вы можете задать число в диапазоне 1024-32767. Если вы откроете порт, отличающийся от порта по умолчанию, вы должны будете указать порт при запуске сценария конфигурирования.

   c. Если вы собираетесь использовать эту систему как хаб, откройте порт 11090, который является портом по умолчанию для защищенных взаимодействий (https).
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Чтобы изменения вступили в силу, заново загрузите определения брандмауэра.
      Введите следующую команду:

      ```
      firewall-cmd --reload
      ```

8. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 2. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 2. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Windows

Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Процедура

1. Установите Windows Server 2016 Standard Edition, согласно инструкциям изготовителя.
2. Измените политики управления учетными записями Windows, выполнив следующие шаги:
    a. Откройте редактор локальной политики защиты, выполнив secpol.msc.
    b. Выберите Локальные политики > Опции защиты и убедитесь, что отключены следующие политики управления учетными записями пользователей:
        - Режим Утверждать администраторов для встроенной учетной записи Администратор
        - Запускать всех администраторов в режиме Утверждать администраторов
3. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
4. Примените обновления Windows и включите дополнительные функции, выполнив следующие шаги:
    a. Примените последние обновления Windows Server 2016.
    b. Установите и включите функцию Windows 2012 R2 Microsoft .NET Framework 3.5 при помощи менеджера сервера Windows.
    c. Если потребуется, обновите драйверы устройств FC и Ethernet HBA до новых уровней.
    d. Установите драйвер ввода-вывода с несколькими путями, соответствующий используемой вами дисковой системе.
5. Откройте порт TCP/IP по умолчанию, 1500, для связи с сервером IBM Spectrum Protect. Например, введите следующую команду:

    ```
    netsh advfirewall firewall add rule name="Backup server port 1500"
    dir=in action=allow protocol=TCP localport=1500
    ```

6. На хаб-сервере Центр операций откройте порт по умолчанию для защищенной (https) связи с компонентом Центр операций. Номер порта - 11090. Например, введите следующую команду:

    ```
    netsh advfirewall firewall add rule name="Центр операций port 11090"
    dir=in action=allow protocol=TCP localport=11090
    ```

Конфигурирование ввода-вывода с несколькими путями

Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.

- Системы AIX
- Системы Linux
- Системы Windows

Системы AIX

Процедура

1. Определите адрес порта Fibre Channel, который нужно использовать для определения хоста в дисковой подсистеме. Введите команду lscfg для каждого порта.
    - В небольших и средних системах введите следующие команды:

        ```
        lscfg -vps -l fcs0 | grep "Network Address"
        lscfg -vps -l fcs1 | grep "Network Address"
        ```

    - В крупных системах введите следующие команды:

        ```
        lscfg -vps -l fcs0 | grep "Network Address"
        lscfg -vps -l fcs1 | grep "Network Address"
        lscfg -vps -l fcs2 | grep "Network Address"
        lscfg -vps -l fcs3 | grep "Network Address"
        ```

2. Убедитесь, что установлены следующие наборы файлов AIX:
    - devices.common.IBM.mpio.rte

- devices.fcp.disk.array.rte
- devices.fcp.disk.rte

3. Введите команду cfgmgr, чтобы система AIX пересканировала оборудование и обнаружила доступные диски. Например:

```
cfgmgr
```

4. Чтобы вызвать список доступных дисков, введите следующую команду:

```
lsdev -Ccdisk
```

Должна появиться выходная информация следующего вида:

```
hdisk0  Доступно 00-00-00 SAS Дисковый накопитель
hdisk1  Доступно 00-00-00 SAS Дисковый накопитель
hdisk2  Доступно 01-00-00 SAS Дисковый накопитель
hdisk3  Доступно 01-00-00 SAS Дисковый накопитель
hdisk4  Доступно 06-01-02 MPIO IBM 2076 Диск ФС
hdisk5  Доступно 07-01-02 MPIO IBM 2076 Диск ФС
...
```

5. Используйте выходную информацию команды lsdev, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

Например, ID устройства может быть `hdisk4`. Сохраните список ID устройств для использования при создании файловых систем для сервера IBM Spectrum Protect.

6. Скоррелируйте ID устройств SCSI с LUN отдельных дисков из дисковой системы, перечислив подробную информацию о всех физических томах в системе. Введите следующую команду:

```
lspv -u
```

В системе IBM® Storwize примером того, что показано для каждого устройства, является следующая информация:

```
hdisk4  00f8cf083fd97327  Нет активен
 332136005076300810105780000000000003004214503IBMfcp
```

В примере значение *600507630081010578000000000000030* - это UID тома, сообщенный интерфейсом управления Storwize.
Чтобы проверить размер дисков (в мегабайтах) и сравнить его с тем, что указано для системы, введите следующую команду:

```
bootinfo -s hdisk4
```

Системы Linux

Процедура

1. Внесите изменения в файл /etc/multipath.conf, чтобы включить поддержку нескольких путей для хостов Linux. Если файл multipath.conf не существует, его можно создать, введя следующую команду:

```
mpathconf --enable
```

В файле multipath.conf при тестировании в системе IBM Storwize были заданы следующие параметры:

```
defaults {
            user_friendly_names no
}

devices {
            device {
                        vendor "IBM "
                        product "2145"
                        path_grouping_policy group_by_prio
                        user_friendly_names no
                        path_selector "round-robin 0"
                        prio "alua"
                        path_checker "tur"
                        failback "immediate"
                        no_path_retry 5
```

```
                        rr_weight uniform
                        rr_min_io_rq "1"
                        dev_loss_tmo 120
                }
}
```

2. Задайте запуск поддержки нескольких путей при запуске системы. Введите следующие команды:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Чтобы убедиться, что диски видны операционной системе и управляются поддержкой нескольких путей, введите следующую команду:

```
multipath -l
```

4. Убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и ID устройств.
   Например, в следующей выходной информации показано, что у диска на 2 ТБ есть две группы путей и четыре активных пути. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула. Используйте часть полного числового ID устройства (в данном примере, 12), чтобы найти том в интерфейсе управления дисковой системой.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
| `- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

   a. Если потребуется, исправьте назначения хостов для LUN диска и произведите принудительное пересканирование шины. Например:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

      Также можно перезапустить систему, чтобы пересканировать назначения хостов для LUN дисков.
   b. Убедитесь, что теперь диски доступны для ввода-вывода по нескольким путям, снова введя команду multipath -l.
5. Используйте выходную информацию команды multipath, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

   Например, ID устройства для вашего диска в 2 ТБ - это `36005076802810c509800000000000012`.

   Сохраните список ID устройств для использования в следующем шаге.

Системы Windows

Процедура

1. Убедитесь, что установлена функция ввода-вывода по нескольким путям. Если потребуется, установите дополнительные драйверы нескольких путей, связанные с поставщиками.
2. Чтобы убедиться, что диски видны операционной системе и управляются вводом-выводом по нескольким путям, введите следующую команду:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Ознакомьтесь с выходной информацией для поддержки нескольких путей и убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и серийных номерах устройств.
   Например, используя часть полного серийного номера устройства (в данном примере, 34), вы сможете искать том в интерфейсе управления дисковой системой. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула хранения.

```
№ УСТР.   4  ИМЯ УСТРОЙСТВА: Disk5 Part0   ТИП: 2145    ПОЛИТИКА: ОПТИМИЗИРОВАННАЯ
СЕР.НОМ.: 600507630081010578000000000000034          РАЗМЕР LUN: 2.0 ТБ
==========================================================================
№ пути       Адаптер/Жесткий диск    Состояние  Режим      Выбор   Ошибки
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Создайте список ID дисковых устройств, используя серийные номера, возвращенные в выходной информации нескольких путей в предыдущем шаге.

   Например, ID устройства для вашего диска в 2 ТБ - это `600507630081010578000000000000034`

   Сохраните список ID устройств для использования в следующем шаге.

5. Чтобы привести новые диски в подключенное состояние и снять атрибут "только для чтения", выполните diskpart.exe со следующими командами. Повторите для каждого из дисков:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Создание ID пользователя для сервера

Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.

Об этой задаче

В ID пользователя можно использовать только буквы в нижнем регистре (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:

- Длина не должна превышать 8 символов.
- ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
- В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

Процедура

1. Чтобы создать ID пользователя, используйте команды операционной системы.
   - Операционные системы AIXОперационные системы LinuxСоздайте группу и ID пользователя в домашнем каталоге пользователя, который станет владельцем экземпляра сервера.

     Например, чтобы создать ID пользователя tsminst1 в группе tsmsrvrs с паролем tsminst1, введите от имени ID административного пользователя следующие команды:

     Операционные системы AIX

     ```
     mkgroup id=1001 tsmsrvrs
     mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
     passwd tsminst1
     ```

     Операционные системы Linux

     ```
     groupadd tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

Выйдите из системы, затем снова в нее войдите. Перейдите на созданную вами учетную запись пользователя. Используйте интерактивную программу входа в систему, например, telnet, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.

-  Операционные системы WindowsСоздайте ID пользователя, а затем добавьте новый ID в группу администраторов. Например, чтобы создать ID пользователя tsminst1, введите следующую команду:

  ```
  net user tsminst1 * /add
  ```

  После создания и проверки пароля для нового пользователя добавьте ID пользователя в группу Администраторы, введя следующие команды:

  ```
  net localgroup Administrators tsminst1 /add
  net localgroup DB2ADMNS tsminst1 /add
  ```

2. Завершите сеанс для нового ID пользователя.

Подготовка файловых систем для сервера

Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

- Подготовка файловых систем в системах AIX
  Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.
- Подготовка файловых систем в системах Linux
  Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.
- Подготовка файловых систем в системах Windows
  Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Подготовка файловых систем в системах AIX

Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.

Процедура

1. Увеличьте глубину очереди и максимальный размер передачи для всех доступных дисков *hdiskX*. Введите для каждого диска следующие команды:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Не выполняйте эти команды для внутренних дисков операционной системы, например, для *hdisk0*.
2. Создайте группы томов для базы данных, активного журнала, архивного журнала, резервного копирования базы данных и пула хранения IBM Spectrum Protect. Введите команду mkvg, указав ID устройств для соответствующих дисков, которые вы указали ранее.
   Например, если имена устройств *hdisk4, hdisk5* и *hdisk6* соответствуют дискам базы данных, включите их в группу томов базы данных и т.д.
   Размер системы: Приведенные ниже команды основаны на конфигурации системы среднего размера. Для малых и больших систем необходимо соответствующим образом настроить синтаксис.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Определите имена физического тома и число свободных физических разделов, которые следует использовать при создании логических томов. Введите команду lsvg для каждой группы томов, которую вы создали в предыдущем шаге.
   Например:

```
lsvg -p tsmdb
```

Вывод будет подобен следующему. В столбце *FREE PPs* представлены свободные физические разделы:

```
tsmdb:
PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active     1631       1631      327..326..326..326..326
hdisk5   active     1631       1631      327..326..326..326..326
hdisk6   active     1631       1631      327..326..326..326..326
```

4. Создайте логические тома в каждой группе томов при помощи команды mklv. Размер томов, группа томов и имена устройств будут разными в зависимости от размера вашей системы и различий в конфигурации дисков. Например, чтобы создать тома для базы данных IBM Spectrum Protect в системе среднего размера, введите следующие команды:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. Сформатируйте файловые системы на каждом логическом томе, используя команду crfs. Например, чтобы сформатировать файловые системы для базы данных в системе среднего размера, введите следующие команды:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Смонтируйте все заново созданные файловые системы, введя следующую команду:

```
mount -a
```

7. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере выходной информации команды показано, что объем используемого пространства, как правило, составляет 1%:

```
tapsrv07> df -g /tsminst1/*
Файловая сист. Блоки ГБ   Свободно  % исп. Мое исп. % моего исп. Смонтировано
/dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
```

8. Убедитесь, что у ID пользователя, созданного вами в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам на сервере.

Подготовка файловых систем в системах Linux

Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.

Процедура

1. Используя список ID устройств, сгенерированный ранее, введите команду mkfs, чтобы создать и сформатировать файловую систему для каждого устройства LUN хранения. Укажите ID устройства в команде. Смотрите следующую таблицу. Для базы данных сформатируйте файловые системы ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
```

Для LUN пула хранения сформатируйте файловые системы xfs:

```
mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
```

Команду mkfs можно вводить до 50 раз в зависимости от того, сколько разных устройств у вас есть.

2. Создайте каталоги точек монтирования для файловых систем.

Введите команду mkdir для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования.

Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

```
mkdir /tsminst1
```

Повторите команду mkdir для каждой файловой системы.

3. Добавьте в файл /etc/fstab запись для каждой файловой системы, чтобы файловые системы монтировались автоматически при запуске сервера.
   Например:

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Смонтируйте файловые системы, которые вы добавили в файл /etc/fstab, введя команду mount -a.
5. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере в системе IBM® Storwize показано, что объем используемого пространства, как правило, составляет 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Файловая сист.                                  Размер Исп. Дост. Исп. % Где смонтир.
/dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
```

6. Убедитесь, что у ID пользователя, созданного вами в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам на сервере IBM Spectrum Protect.

Подготовка файловых систем в системах Windows

Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Процедура

1. Создайте каталоги точек монтирования для файловых систем.
   Введите команду md для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования. Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

```
md c:\tsminst1
```

   Повторите команду md для каждой файловой системы.
2. Создайте том для каждого LUN диска, отображенного в каталог в каталоге экземпляра сервера с использованием менеджера томов Windows.

   Выберите Менеджер серверов > Службы файлов и хранения и выполните описанные ниже шаги для каждого диска, соответствующего отображению LUN, созданному в предыдущем шаге:

   a. Переведите диск в подключенное состояние.
   b. Инициализируйте диск до базового типа GPT, который является типом по умолчанию.
   c. Создайте простой том, занимающий все пространство на диске. Сформатируйте файловую систему с использованием NTFS и задайте метку, соответствующую назначению тома, например, TSMfile00. Не назначайте для нового тома букву диска. Вместо этого отобразите том в каталог в каталоге экземпляра, например, в C:\tsminst1\TSMfile00.
      Совет: Определите метку тома и метки отображений каталога на основе сообщенного размера диска.
3. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Вызовите список всех файловых систем, введя команду mountvol и ознакомившись с выходной информацией. Например:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
  C:\tsminst1\TSMdbspace00\
```

4. По завершении конфигурирования диска перезапустите систему.

Дальнейшие действия

Вы можете подтвердить объем свободного пространства для каждого тома, используя Проводник Windows.

Установка сервера и компонента Центр операций

Используйте для установки компонентов графический мастер IBM® Installation Manager.

- Установка в системах AIX и Linux
  Установите сервер IBM Spectrum Protect и Центр операций в той же системе.
- Установка в системах Windows
  Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Установка в системах AIX и Linux

Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Прежде чем начать

Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

1. Операционные системы AIXУбедитесь, что у вас в системе установлены необходимые файлы RPM.

   Дополнительные сведения смотрите в разделе Установка обязательных файлов RPM для графического мастера.

2. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042992.
3. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
4. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

   ```
   chmod a+x имя_пакета.bin
   ```

5. Извлеките пакет, введя следующую команду:

   ```
   ./имя_пакета.bin
   ```

   где *имя_пакета* - это имя скачанного файла.
6. Операционные системы AIXУбедитесь, что включена следующая команда, чтобы мастера работали правильно:

   ```
   lsuser
   ```

   По умолчанию эта команда включена.
7. Перейдите в каталог, куда вы поместили исполняемый файл.
8. Запустите мастер установки, введя следующую команду:

   ```
   ./install.sh
   ```

   Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

- Установка обязательных файлов RPM для графического мастера
  Файлы RPM необходимы для графического мастера IBM Installation Manager.

Задачи, связанные с данной:
Другие методы установки компонентов IBM Spectrum Protect (AIX)
Другие методы установки компонентов IBM Spectrum Protect (Linux)

Установка в системах Windows

Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Прежде чем начать

Убедитесь, что выполнены следующие обязательные требования:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
- Убедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

1. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042993.
2. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
3. Перейдите в каталог, куда вы поместили исполняемый файл.
4. Дважды щелкните по выполняемому файлу, чтобы извлечь его в текущий каталог.
5. В каталоге, куда были распакованы файлы установки, запустите мастер установки, дважды щелкнув по файлу install.bat. Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager.

  Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Задачи, связанные с данной:
Другие методы установки компонентов IBM Spectrum Protect

Конфигурирование сервера и компонента Центр операций

После установки компонентов выполните конфигурирование сервера IBM Spectrum Protect и компонента Центр операций.

- Конфигурирование экземпляра сервера
  Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.
- Установка клиента резервного копирования и архивирования
  Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.
- Как задать опции для сервера
  Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.

- Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)
  Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.
- Конфигурирование Центра операций
  После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.
- Регистрация лицензии на продукт
  Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.
- Конфигурирование дедупликации данных
  Создайте пул хранения каталогов-контейнеров и хотя бы один каталог пула хранения, чтобы использовать встроенную дедупликацию данных.
- Как задать правила хранения данных для вашего бизнеса
  После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.
- Как задать расписания для операций по обслуживанию сервера
  Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.
- Определение расписаний клиентов
  Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Конфигурирование экземпляра сервера

Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.

Прежде чем начать

Убедитесь, что выполнены следующие требования:
Операционные системы AIXОперационные системы Linux

- В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
- В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле sshd_config в каталоге /etc/ssh/. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения *localhost*.
- Вы должны иметь возможность войти в IBM Spectrum Protect, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
- Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Операционные системы WindowsУбедитесь, что служба удаленного реестра запущена, выполнив следующие шаги:

1. Выберите Пуск > Администрирование > Службы. В окне Службы выберите Удаленный реестр. Если служба не запущена, щелкните по Пуск.
2. Убедитесь, что порты 137, 139 и 445 не заблокированы брандмауэром:
   a. Щелкните по Запуск > Панель управления > Брандмауэр Windows.
   b. Выберите Дополнительные параметры.
   c. Выберите Входные правила.
   d. Выберите Новое правило.
   e. Создайте правило порта для портов TCP 137, 139 и 445, чтобы разрешить соединения для доменных и частных сетей.
3. Сконфигурируйте управление учетными записями пользователей, получив доступ к опциям Локальная политика безопасности и выполнив следующие шаги:
   a. Щелкните по Пуск > Администрирование > Локальная политика безопасности. Разверните Локальные политики > Опции безопасности.
   b. Если эта возможность еще не включена, включите встроенную учетную запись администратора, выбрав Учетные записи: Состояние учетной записи администратора > Включить > ОК.

c. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для всех администраторов Windows, выбрав Управление учетными записями пользователей: Запускать всех администраторов в режиме утверждения администраторов > Выключить > ОК.
d. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для встроенной учетной записи администратора, выбрав Управление учетными записями пользователей: Режим утверждения администраторов для встроенной учетной записи администратора > Выключить > ОК.

4. Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Об этой задаче

Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

Процедура

1. Запустите локальную версию мастера.
   - Операционные системы AIXОперационные системы LinuxОткройте программу dsmicfgx в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запустить только от имени пользователя root.
   - Операционные системы WindowsЩелкните по Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования.
2. Завершите конфигурирование, следуя инструкциям. Используйте информацию, записанную вами в таблицу Рабочие листы планирования в ходе настройки системы IBM Spectrum Protect, чтобы задать каталоги и опции в мастере.

   Операционные системы AIXОперационные системы LinuxВ окне Информация о сервере задайте автоматический запуск сервера при загрузке системы, используя ID пользователя экземпляра.

   Операционные системы WindowsПри использовании мастера конфигурирования для сервера будет задан автоматический запуск при перезагрузке.

Установка клиента резервного копирования и архивирования

Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.

Процедура

Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.

- Установить клиентов резервного копирования и архивирования UNIX и Linux
- Первая установка клиента Windows

Как задать опции для сервера

Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.

Процедура

1. Перейдите в каталог экземпляра сервера и откройте файл dsmserv.opt.
2. Ознакомьтесь со следующими значениями в таблице и проверьте параметры опций сервера на основе размера системы.

Серверный параметр	**Значение для небольшой системы**	**Значение для средней системы**	**Значение для крупной системы**
ACTIVELOGDIRECTORY	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации

Серверный параметр	Значение для небольшой системы	Значение для средней системы	Значение для крупной системы
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Да	Нет	Нет
ARCHLOGDIRECTORY	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	Нет	Нет	Нет
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Обновите параметры опций сервера, если потребуется, чтобы они соответствовали значениям в таблице. Чтобы внести обновления, закройте файл dsmserv.opt и воспользуйтесь командой SETOPT в интерфейсе командной строки администрирования, чтобы задать опции.
Например, чтобы обновить опцию IDLETIMEOUT до 60, введите следующую команду:

```
setopt idletimeout 60
```

3. Чтобы сконфигурировать защищенную связь с сервером, клиентами и Центр операций, то проверьте опции в следующей таблице:

Серверный параметр	Системы всех размеров
SSLFIPSMODE	NO
TCPPORT	Задайте номер порта, на котором сервер ожидает требований установления сеансов TCP/IP и SSL от клиента.
TCPADMINPORT	Задайте адрес порта, на котором сервер ожидает требований установления сеансов TCP/IP и SSL от клиента администрирования с интерфейсом командной строки.

Если нужно обновить любое из значений опций, измените файл dsmserv.opt, используя следующие рекомендации:
- Чтобы включить опцию, удалите звездочку в начале строки.
- В каждой строке введите только одну опцию и заданное для нее значение.
- Если опция встречается в нескольких записях в файле, сервер будет использовать последнюю запись.

Сохраните свои изменения файл и закройте файл. Если вы непосредственно внесете изменения в файл dsmserv.opt, вы должны будете перезапустить сервер, чтобы изменения вступили в силу.

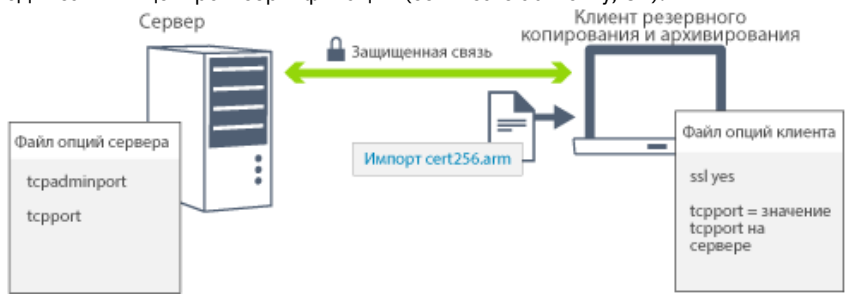
Ссылки, связанные с данной:
Справочник по опциям сервера
SETOPT (Задать динамическое обновление серверной опции)

Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)

Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.

Об этой задаче

Как показано на следующем рисунке, вы можете вручную сконфигурировать защищанную связь между сервером и клиентом резервного копирования и архивирования, задав опции в файлах опций сервера и клиента, а затем перенеся на клиент самоподписанный сертификат, сгенерированный на сервере. Либо можно получить уникальный сертификат, подписанный центром сертификации (certificate authority, CA).



Дополнительную информацию о конфигурировании сервера и клиентов для взаимодействий SSL или TLS смотрите в разделе Конфигурирование агентов хранения, серверов, клиентов и центра операций для соединения с сервером с использованием SSL.

Конфигурирование Центра операций

После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.

Прежде чем начать

Если вы подключаетесь к компоненту Центр операций впервые, вы должны предоставить следующую информацию:

- Информация о соединении для сервера, который вы хотите назначить хаб-сервером
- Идентификационные данные входа в систему для администратора, который задан для этого сервера

Процедура

1. Определите хаб-сервер. Введите в окне веб-браузера следующий адрес:

   `https://`*`имя_хоста`*`:`*`защищенный_порт`*`/oc`

   Здесь используются следующие обозначения:
   - *имя_хоста* - это имя компьютера, где установлен компонент Центр операций
   - *защищенный_порт* - это номер порта, используемого компонентом Центр операций для HTTPS-взаимодействий на этом компьютере

   Например, если имя хоста - это tsm.storage.mylocation.com и вы используете для компонента Центр операций защищенный порт по умолчанию, адрес пример следующий вид:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

   Когда вы впервые входите в компонент Центр операций, мастер поможет вам выполнить первоначальное конфигурирование, чтобы задать нового администратора с системными полномочиями на сервере.

2. Настройте защищенные взаимодействия между компонентом Центр операций и хаб-сервером, сконфигурировав протокол Secure Sockets Layer (SSL).

   Следуйте инструкциям в разделе Защита связи между компонентом Центр операций и хаб-сервером.

3. Необязательно: Чтобы ежедневно получать по электронной почте отчет, в котором суммируется состояние системы, сконфигурируйте параметры электронной почты в компоненте Центр операций.

   Следуйте инструкциям в разделе Состояние системы отслеживания с использованием отчетов по электронной почте.

- Защита связи между компонентом Центр операций и хаб-сервером
  Для защиты связи между компонентом Центр операций и хаб-сервером добавьте сертификат Transport Layer

Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Регистрация лицензии на продукт

Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.

Об этой задаче

Лицензии хранятся в файлах сертификата регистрации, который содержит сведения о лицензировании для продукта. Файлы регистрационных сертификатов находятся на носителе установки и при установке помещаются на сервер. После регистрации продукта лицензии хранятся в NODELOCK-файле в текущем каталоге.

Процедура

Зарегистрируйте лицензию, указав имя файла сертификата регистрации, содержащего лицензию. Чтобы использовать построитель команд Центр операций для этой задачи, выполните следующие шаги:

1. Откройте Центр операций.
2. Откройте построитель команд компонента Центр операций, установив указатель мыши на значок параметров и щелкнув по Построитель команд.
3. Введите команду REGISTER LICENSE. Например, чтобы зарегистрировать базовую лицензию IBM Spectrum Protect, введите следующую команду:

```
register license file=tsmbasic.lic
```

Дальнейшие действия

Сохраните носитель установки, на котором содержатся файлы сертификата регистрации. Возможно, вам придется снова зарегистрировать лицензию, если, например, возникнет одно из следующих условий:

- Сервер перенесен на другой компьютер;
- Файл NODELOCK поврежден. Сервер сохраняет данные лицензий в файле NODELOCK, расположенном в каталоге, из которого запускается сервер.
- Операционные системы LinuxВы изменяете микросхему процессора, связанную с сервером, на котором установлен сервер.

Ссылки, связанные с данной:
REGISTER LICENSE (регистрация новой лицензии)

Конфигурирование дедупликации данных

Создайте пул хранения каталогов-контейнеров и хотя бы один каталог пула хранения, чтобы использовать встроенную дедупликацию данных.

Прежде чем начать

Используйте при выполнении этой задачи информацию о каталоге пула хранения данных, которую вы записали в разделе Рабочие листы планирования.

Процедура

1. Откройте Центр операций.
2. В строке меню Центр операций установите указатель мыши на Хранилище.
3. В появившемся списке щелкните по Пулы хранилищ.
4. Щелкните по кнопке + Пул хранилищ.
5. Выполните шаги в мастере Добавить пул хранения:
    - Чтобы использовать встроенную дедупликацию данных, выберите пул хранения Каталог в хранилище на основе контейнеров.
    - При конфигурировании каталогов для пула хранения каталогов-контейнеров задайте пути каталогов, которые вы создали для хранения во время настройки системы.

6. После того как вы сконфигурируете новый пул хранения каталогов-контейнеров, щелкните по Закрыть и просмотреть политики, чтобы обновить класс управления и начать использовать пул хранения.

Как задать правила хранения данных для вашего бизнеса

После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.

Процедура

1. На странице Службы в Центр операций выберите домен STANDARD и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики. На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.
3. Щелкните по переключателю Конфигурировать и внесите следующие изменения:
   - Измените объект назначения резервного копирования для класса управления STANDARD, задав пул хранения каталога-контейнера.
   - Измените значение в столбце Резервные копии на Без ограничения.
   - Измените срок хранения. Задайте в столбце Хранить лишние резервные копии значение 30 дней или более в зависимости от ваших бизнес-требований.
4. Сохраните изменения и щелкните по переключателю Конфигурировать, чтобы набор политик стал недоступен для изменения.
5. Активируйте набор политик, для чего щелкните по Активировать.

Задачи, связанные с данной:
Как задать роли для резервного копирования и архивирования данных клиента

Как задать расписания для операций по обслуживанию сервера

Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.

Об этой задаче

Запланируйте операции обслуживания сервера, так чтобы они выполнялись после операций резервного копирования клиента. Вы можете управлять синхронизацией расписаний, задав время начала в сочетании с длительностью каждой операции.

В приведенном ниже примере показано, как можно запланировать операции обслуживания сервера в сочетании с расписанием резервного копирования клиента для дискового решения с одной площадкой.

Операция	**Запланированное задание**
Резервное копирование клиента	Начинается в 22:00.
Обработка базы данных и файлов аварийного восстановления	• Операция резервного копирования базы данных начинается в 11:00 или через 13 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения. • Информация о конфигурации устройства и резервное копирование хронологии томов запускаются в 17:00 или спустя 6 часов после запуска операций резервного копирования базы данных. • Удаление хронологии томов запускается в 20:00 или спустя 9 часов после запуска операции резервного копирования базы данных.
Устаревание инвентарного перечня	Начинается в 12:00 или через 14 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения.

Процедура

После того как вы сконфигурируете класс устройств для резервных копий базы данных, создайте расписания для резервного копирования базы данных и других необходимых операций обслуживания, используя команду DEFINE

SCHEDULE. В зависимости от размера вашей среды вам, возможно, придется скорректировать время запуска для каждого расписания в примере.

1. Определить класс устройства для операций резервного копирования. Например, используйте команду DEFINE DEVCLASS, чтобы создать класс устройств с именем DBBACK_FILEDEV:

   ```
   define devclass dbback_filedev devtype=file
     directory=каталоги_резервных_копий_бд
   ```

   где *каталоги_резервных_копий_бд* - это список каталогов, которые вы создали для резервных копий базы данных. Операционные системы AIXОперационные системы LinuxНапример, если у вас есть четыре каталога для резервных копий базы данных, начиная с /tsminst1/TSMbkup00, введите следующую команду:

   ```
   define devclass dbback_filedev devtype=file
     directory=/tsminst1/TSMbkup00,
     /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
     /tsminst1/TSMbkup03"
   ```

   Операционные системы WindowsНапример, если у вас есть четыре каталога для резервных копий базы данных, начиная с C:\tsminst1\TSMbkup00, введите следующую команду:

   ```
   define devclass dbback_filedev devtype=file
     directory="c:\tsminst1\TSMbkup00,
     c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
   ```

2. Задайте класс устройств для операций автоматического резервного копирования базы данных. Используйте команду SET DBRECOVERY, чтобы указать класс устройств, созданный вами в предыдущем шаге. Например, если класс устройств - это dbback_filedev, введите следующую команду:

   ```
   set dbrecovery dbback_filedev
   ```

3. Создайте расписания для операций обслуживания, используя команду DEFINE SCHEDULE. Обязательные операции с примерами команд смотриет в следующей таблице.

Операция	**Пример команды**
Создайте резервную копию базы данных.	Создайте расписание, чтобы выполнить команду BACKUP DB. Если вы конфигурируете небольшую систему, задайте для параметра COMPRESS значение YES. Например, в небольшой системе введите следующую команду, чтобы создать расписание резервного копирования, использующее новый класс устройств: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Создать рез. копию базы данных." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Создайте резервную копию информации о конфигурации устройств.	Создайте расписание, чтобы выполнить команду BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Создать рез. копию файла конфигурации устройства." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Создайте резервную копию хронологии томов.	Создайте расписание, чтобы выполнить команду BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Создать резервную копию хронологии томов." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

Операция	Пример команды
Удалите более старые версии резервных копий базы данных, которые больше не требуются.	Создайте расписание, чтобы выполнить команду DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Удалить старые резервные копии базы данных." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Удалите объекты, у которых превышен допустимый срок хранения.	Создайте расписание, чтобы выполнить команду EXPIRE INVENTORY. Задайте параметр RESOURCE на основе размера системы, которую вы конфигурируете: ○ Небольшие системы: 10 ○ Средние системы: 30 ○ Крупные системы: 40 Например, в системе среднего размера, введите следующую команду, чтобы создать расписание с именем EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Удалить проср. объекты." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Дальнейшие действия

После того как вы создадите расписания задач по обслуживанию сервера, вы сможете увидеть их в компоненте Центр операций, выполнив следующие шаги:

1. В строке меню Центр операций установите указатель мыши на Серверы.
2. Щелкните по Обслуживание.

Ссылки, связанные с данной:
DEFINE SCHEDULE (определение расписания выполнения административных команд)

Определение расписаний клиентов

Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Процедура

1. В строке меню Центр операций установите указатель мыши на Клиенты.
2. Щелкните по Расписания.
3. Щелкните по + Расписание.
4. Выполните шаги в мастере Создать расписание. Задайте запуск расписаний резервного копирования клиента в 22:00, основываясь на операциях по обслуживанию сервера, которые вы запланировали в разделе Как задать расписания для операций по обслуживанию сервера.

Установка и конфигурирование клиентов резервного копирования и архивирования

После успешной настройки системы сервера IBM Spectrum Protect установите и сконфигурируйте программу клиента, чтобы начать резервное копирование данных.

Процедура

Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.

- Установить клиентов резервного копирования и архивирования UNIX и Linux
- Первая установка клиента Windows

Дальнейшие действия

Зарегистрируйте свои клиенты и назначьте их для расписаний.

- Регистрация и назначение клиентов в расписания
  Добавьте и зарегистрируйте клиенты при помощи компонента Центр операций, воспользовавшись мастером Добавить клиент.
- Установка службы управления клиентом
  Установите службу управления клиентом для клиентов резервного копирования и архивирования, работающих в операционных системах Linux и Windows. Служба управления клиентом собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает эту информацию доступной для компонента Центр операций для базовой возможности мониторинга.

Регистрация и назначение клиентов в расписания

Добавьте и зарегистрируйте клиенты при помощи компонента Центр операций, воспользовавшись мастером Добавить клиент.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию technote 7048963.
Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе Аутентификация пользователей с использованием базы данных Active Directory.

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды REGISTER NODE и задайте параметр USERID:

  ```
  register node имя_узла пароль userid=имя_узла
  ```

  где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе Регистрация узла.
- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центр операций. Сделайте следующее:
  a. В панели меню Центра операций выберите Клиенты.
  b. В таблице Клиенты щелкните по + Клиент.
  c. Выполните шаги в мастере Добавить клиент:
     i. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель Включить в области Дедупликация данных на стороне клиента.
     ii. В окне Конфигурация скопируйте значения TCPSERVERADDRESS, TCPPORT, NODENAME, и DEDUPLICATION.
     Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
     iii. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     iv. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     v. Щелкните по Добавить клиент.

Установка службы управления клиентом

Установите службу управления клиентом для клиентов резервного копирования и архивирования, работающих в операционных системах Linux и Windows. Служба управления клиентом собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает эту информацию доступной для компонента Центр операций для базовой возможности мониторинга.

Процедура

Установите службу управления клиентом на том же компьютере, на котором находится клиент резервного копирования и архивирования, выполнив следующие шаги:

1. Скачайте пакет установки службы управления клиентом с сайта скачиваемых материалов IBM®, например, с сайта IBM Passport Advantage® или IBM Fix Central. Ищите имя файла, аналогичное следующему: `<версия>-IBM_Spectrum_Protect-CMS-операционная_система.bin`.
2. Создайте каталог на компьютере клиента, которым вы хотите управлять, и скопируйте в него пакет установки.
3. Распакуйте контент файла пакета установки.
4. Запустите пакетный файл установки из каталога, в который вы распаковали файлы установки и связанные файлы. Это каталог, который вы создали на шаге 2.
5. Чтобы установить службу управления клиентом, выполните инструкции в мастере IBM Installation Manager. Если на компьютере клиента еще не установлен компонент IBM Installation Manager, вы должны выбрать и IBM Installation Manager, и службу управления клиентом IBM Spectrum Protect.

- Проверка того, правильно ли установлена служба управления клиентами
  Прежде чем использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, вы можете убедиться, что служба управления клиентом правильно установлена и сконфигурирована.
- Конфигурирование Центр операций на использование службы управления клиентом
  Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Задачи, связанные с данной:
Конфигурирование службы управления клиентами для пользовательских установок клиентов

Проверка того, правильно ли установлена служба управления клиентами

Прежде чем использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, вы можете убедиться, что служба управления клиентом правильно установлена и сконфигурирована.

Процедура

Введите на компьютере клиента в командной строке следующие команды, чтобы посмотреть конфигурацию службы управления клиентом:

- На компьютерах клиента Linux введите следующую команду:

  ```
  каталог_установки_клиента/cms/bin/CmsConfig.sh
  list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

```
    Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- На компьютерах клиента Windows введите следующую команду:

  ```
  каталог_установки_клиента\cms\bin\CmsConfig.bat list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Если служба управления клиентами правильно установлена и сконфигурирована, то в выходных результатах показан каталог файла журнала ошибок.
Выходной текст извлекается из следующего файла конфигурации:

- На компьютерах клиента Linux:

  ```
  каталог_установки_клиента/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- На компьютерах клиента Windows:

  ```
  каталог_установки_клиента\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
  ```

Если в выходных результатах нет ни одной записи, то нужно сконфигурировать файл client-configuration.xml. Инструкции по конфигурированию этого файла смотрите в разделе Конфигурирование службы управления клиентами для пользовательских установок клиентов. Можно использовать команду CmsConfig verify, чтобы проверить, правильно ли создано определение узла в файле client-configuration.xml.

Конфигурирование Центр операций на использование службы управления клиентом

Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Прежде чем начать

Убедитесь, что служба управления клиентом установлена и запущена на компьютере клиента. Проверьте, используется ли конфигурация по умолчанию. Конфигурация по умолчанию не используется в следующих случаях:

- Служба управления клиентом не использует номер порта по умолчанию (9028).
- Для клиента резервного копирования и архивирования не используется IP-адрес, который используется для компьютера клиента резервного копирования и архивирования. Например, другой IP-адрес может использоваться в следующих случаях:
  - В компьютерной системе установлено две сетевые карты. Клиент резервного копирования и архивирования сконфигурирован для взаимодействия с одной сетью, а служба управления клиентом взаимодействует с другой сетью.
  - На компьютере клиента используется DHCP. Поэтому компьютеру клиента динамически назначается IP-адрес, сохраненный на сервере во время предыдущей операции клиента резервного копирования и архивирования. При перезагрузке компьютера клиента ему может быть назначен другой IP-адрес. Чтобы Центр операций всегда мог найти компьютер клиента, нужно задать полное имя домена.

Процедура

Чтобы сконфигурировать Центр операций для использования службы управления клиентом, сделайте следующее:

1. Выберите клиента на странице Клиенты Центра операций.
2. Выберите Сведения > Свойства.
3. В поле URL удаленной диагностики в разделе Общие задайте URL для службы управления клиентом в системе клиента. Адрес должен начинаться с `https`. В следующей таблице показаны примеры URL удаленной диагностики.

Тип URL	Пример
С именем хоста DNS и портом по умолчанию (9028)	https://server.example.com
С именем хоста DNS и портом не по умолчанию	https://server.example.com:1599
С IP-адресом и портом не по умолчанию	https://192.0.2.0:1599

4. Щелкните по Сохранить.

Дальнейшие действия

Вы можете получить доступ к диагностической информации о клиенте (например, к файлам журнала клиента) на вкладке Диагностика в Центре операций.

Завершение реализации

После того, как решение IBM Spectrum Protect будет сконфигурировано и заработает, проверьте операции резервного копирования и настройте мониторинг, чтобы убедиться, что все нормально работает.

Процедура

1. Проверьте операции резервного копирования, чтобы убедиться, что ваши данные защищены, как вы и ожидали.
   a. Выберите на странице Клиенты компонента Центр операций клиенты, для которых вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
   b. На странице Серверы в компоненте Центр операций выберите сервер, для которого вы хотите производить резервное копирование базы данных. Щелкните по Резервное копирование и выполните инструкции в окне Резервное копирование базы данных.
   c. Убедитесь, что резервное копирование выполнено без предупреждений или сообщений об ошибках.
   Совет: Либо можно использовать графический интерфейс клиента резервного копирования и архивирования для резервного копирования данных клиента, и можно производить резервное копирование базы данных, вводя команду BACKUP DB из административной командной строки.
2. Настройте мониторинг для ваших решений, следуя инструкциям в разделе Мониторинг решения с одной площадкой.

Мониторинг решения с одной площадкой

После реализации дискового решения IBM Spectrum Protect с одной площадкой произведите мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.

Об этой задаче

Предпочтительный способ мониторинга решения заключается в использовании компонента Центр операций, который позволяет получить общее и подробное состояние системы в графическом пользовательском интерфейсе. Кроме того, можно сконфигурировать центр операций для генерирования ежедневного отчета по электронной почте, в котором суммируется состояние системы.

В некоторых случаях для выполнения отдельных задач по мониторингу или устранению ошибок вам может потребоваться использовать расширенные инструменты мониторинга.

Совет: Если вы собираетесь диагностировать проблемы клиентов резервного копирования и архивирования в операционных системах Linux или Windows, установите службу управления клиентом IBM Spectrum Protect на каждом

компьютере, где установлен клиент резервного копирования и архивирования. Таким образом можно обеспечить нахождение кнопки Диагностика в компоненте Центр операций для диагностики проблем клиентов резервного копирования и архивирования. Чтобы установить службу управления клиентом, выполните инструкции в разделе Установка службы управления клиентом.

Процедура

1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе Контрольный список ежедневного мониторинга.
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе Контрольный список периодического мониторинга.
3. Чтобы проверить, соответствует ли ваше решение IBM Spectrum Protect требованиям по лицензированию, следуйте инструкциям в разделе Проверить соответствие лицензии.
4. Как сконфигурировать центр операций для генерирования отчетов о состоянии электронной почты, смотрите в разделе Состояние системы отслеживания с использованием отчетов по электронной почте

Дальнейшие действия

Устраните все обнаруженные вами проблемы. Чтобы устранить проблему, изменив конфигурацию вашего решения, следуйте инструкциям в разделе Управление операциями для дискового решения с одной площадкой. Кроме того, существуют следующие ресурсы:

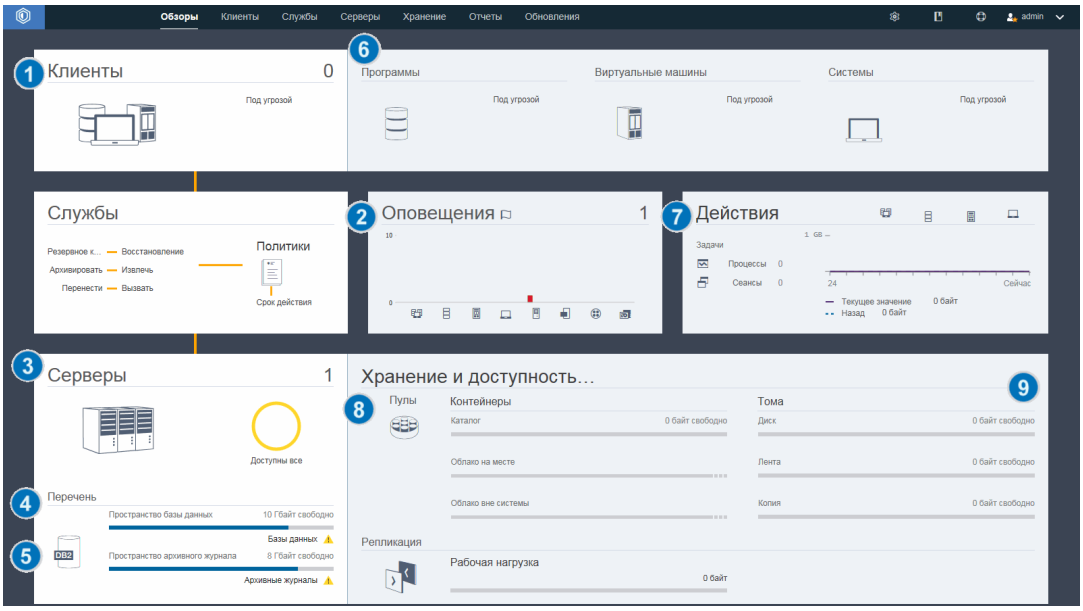
- Информацию об устранении проблем производительности смотрите в разделе Производительность.
- Информацию об устранении других проблем смотрите в разделе Устранение неполадок.

Контрольный список ежедневного мониторинга

Чтобы убедиться, что вы выполняете ежедневные задачи мониторинга для своего решения IBM Spectrum Protect, ознакомьтесь с ежедневным контрольным списком для мониторинга.

Выполняйте ежедневные задачи мониторинга со страницы Обзор в компоненте Центр операций. Доступ к странице Обзор можно получить, открыв Центр операций и щелкнув по Обзоры.

На рисунке ниже показано расположение для завершения каждой операции.



Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

В следующей таблице перечислены ежедневные задачи мониторинга и представлены инструкции по выполнению каждой задачи.

Табл. 1. Задачи ежедневного мониторинга

Задача	**Основные процедуры**	**Дополнительные процедуры и диагностическая информация**
Наблюдайте за уведомлениями о защите, которые могут указывать на атаку программы-вымогателя.	Если потенциальная атака программы-вымогателя обнаружена в среде IBM Spectrum Protect, то будет показано уведомление о защите на переднем плане Центр операций. Дополнительную информацию можно получить, щелкнув по сообщению, чтобы открыть страницу Уведомления о защите.	На странице Уведомления о защите можно выполнить следующие действия: • Просмотр подробностей уведомления по клиентам. Ограничение: В Центр операций версии 8.1.5, уведомления доступны только для клиентов резервного копирования-архивирования. • Подтвердите уведомление защиты, выбрав его и щелкнув по Подтвердить. При подтверждении уведомления о защите в столбец Подтверждение на странице Уведомления о защите добавляется символ галочки для выбранного клиента. Стандарт, по которому подтверждается уведомление, определяется в вашей организации. Галочка может означать, что вы исследовали проблему и решили, что это - ложное положительное. Это также может означать, что проблема существует, и она решается. • Назначьте уведомление о защите администратору, выбрав уведомление о защите и нажав Назначить. Чтобы рассмотреть назначение, администратор должен зарегистрироваться в Центр операций и щелкнуть Обзоры > Защита. Если вы не уверены, что администратор регулярно отслеживает страницу Уведомления о защите, сообщите администратору о назначении. • Если уведомление - ложное положительное, то можно выбрать уведомление о защите и щелкните по Сброс. Уведомление о защите удалено. Хронологические данные, используемые для базовых сравнений с самой последней операцией резервного копирования, удаляются. С этого момента вычисляется новая базовая линия.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
1 Определите, подвергаются ли клиенты риску оказаться незащищенными из-за неудавшихся или пропущенных операций резервного копирования.	Чтобы проверить, находятся ли клиенты под угрозой, в области Клиенты найдите уведомление Под угрозой. Чтобы просмотреть сведения, щелкните по области Клиенты. Внимание: Если процент Под угрозой намного больше обычного, то это может указывать на атаку программы-вымогателя. Атака программы-вымогателя может привести к сбоям резервного копирования, тем самым создавая риск для клиентов. Например, если процент клиентов в опасности обычно между 5% и 10%, но процент увеличивается до 40% или 50%, то изучите причину этого. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете увидеть и проанализировать ошибку клиента и запланировать журналы, выполнив следующие шаги: 1. В таблице Клиенты выберите клиент и щелкните по Сведения. 2. Чтобы диагностировать проблему, щелкните по Диагноз.	В случае клиентов, у которых нет установленной службы управления клиентом, получите доступ к системе клиента, чтобы проверить журналы ошибок клиента.
2 Определите, нужно ли уделить внимание ошибкам клиента или сервера.	Чтобы определить серьезность всех оповещений, о которых было сообщено, установите указатель мыши на столбцы в области Оповещения.	Чтобы увидеть дополнительную информацию об оповещениях, выполните следующие шаги: 1. Щелкните по области Оповещения. 2. В таблице Оповещения выберите оповещение. 3. В панели Журнал операций просмотрите сообщения. В панели показаны связанные сообщения, созданные до и после возникновения выбранного оповещения.
3 Определите, доступны ли серверы, которыми управляет Центр операций, для предоставления клиентам служб по защите данных.	1. Чтобы проверить, находятся ли серверы под угрозой, в области Серверы найдите уведомление Недоступен. 2. Чтобы увидеть дополнительную информацию, щелкните по области Серверы. 3. Выберите сервер в таблице Серверы и щелкните по Сведения.	Совет: Если вы обнаружите проблему, связанную со свойствами сервера, обновите свойства сервера: 1. В таблице Серверы выберите сервер и щелкните по Сведения. 2. Чтобы обновить свойства сервера, щелкните по Свойства.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
4 Определите, доступно ли достаточно пространства для перечня сервера, состоящего из базы данных сервера, активного журнала и архивного журнала.	1. Щелкните по области Серверы. 2. В столбце Состояние в таблице проверьте состояние сервера и устраните все ошибки: ○ Нормальное Для базы данных сервера, активного журнала и архивного журнала доступен достаточный объем пространства. ○ Критическое Для базы данных сервера, активного журнала или архивного журнала недостаточно пространства. Нужно немедленно добавить пространство, иначе работа служб защиты данных, предоставляемых сервером, будет прервана. ○ Предупреждение , В базе данных сервера, активном журнале или архивном журнале заканчивается пространство. Если это условие повторяется, то нужно добавить пространство. ○ Недоступно Невозможно получить состояние. Убедитесь, что сервер работает и что в сети нет ошибок. Это состояние показывается также, если ID администратора мониторинга заблокирован или недоступен на сервере по другой причине. Значение этого ID - IBM-OC-имя_хаб-сервера. ○ Неотслеживаемый Неотслеживаемые серверы заданы на хаб-сервере, но не сконфигурированы для управления компонентом Центр операций. Чтобы сконфигурировать не отслеживаемый сервер, выберите сервер и щелкните по Отслеживать подчиненный.	Можно также просмотреть связанные оповещения на странице Оповещения. Дополнительную информацию об устранении ошибок смотрите в разделе Устранение проблем сервера.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
5 Проверьте операции резервного копирования базы данных.	Чтобы определить, когда в последний раз производилось резервное копирование сервера, выполните следующие шаги: 1. Щелкните по области Серверы. 2. В таблице Серверы проверьте столбец Последнее резервное копирование базы данных.	Чтобы получить более подробную информацию об операциях резервного копирования, выполните следующие шаги: 1. В таблице Серверы выберите строку и щелкните по Сведения. 2. В области Резервное копирование БД установите указатель мыши на галочки, чтобы прочесть информацию об операциях резервного копирования. Если резервное копирование базы данных не производилось недавно (например, за последние 24 часа), вы можете запустить операцию резервного копирования: 1. На странице Обзор в компоненте Центр операций щелкните по области Серверы. 2. В таблице выберите сервер и щелкните по Резервное копирование. Чтобы определить, сконфигурирована ли база данных сервера для автоматических операций резервного копирования, выполните следующие шаги: 1. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY DB: `query db f=d` 3. В выходной информации проверьте значение в поле `Полное имя класса устройств`. Если класс устройства указан, это означает, что сервер сконфигурирован для автоматического резервного копирования базы данных.
6 Отслеживайте другие задачи по обслуживанию сервера. Задачи по обслуживанию сервера могут включать в себя выполнение расписаний административных команд, сценариев обслуживания и связанных команды.	Чтобы найти информацию о процессах, которые завершились неудачно из-за проблем на сервере, выполните следующие шаги: 1. Выберите Серверы > Обслуживание. 2. Чтобы получить двухнедельную хронологию процесса, смотрите столбец Хронология. 3. Чтобы получить больше информации о запланированном процессе, установите указатель мыши на переключателее, связанном с процессом.	Более подробную информацию о процессах мониторинга и устранении проблем смотрите в электронной справке компонента Центр операций.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
7 Убедиться, что объем данных, переданных на серверы и полученных с них, находится в ожидаемом диапазоне.	• Чтобы получить обзор операций за последние 24 часа, смотрите область Операции. • Чтобы сравнить активность за последние 24 часа с активностью за предыдущие 24 часа, смотрите показатели в областях Текущие и Предыдущие.	• Если на сервер было отправлено больше данных, чем вы ожидали, определите, какие клиенты создают резервные копии большего объема данных, и исследуйте причину. Возможно, что дедупликация данных на стороне клиента работает неправильно. Внимание: Если объем резервных данных значительно больше обычного, то это может указывать на атаку программы-вымогателя. Когда программа-вымогатель шифрует данные, система обнаруживает, что данные изменяются и что резервная копия создается для измененных данных. Тем самым тома резервного копирования становятся больше. Чтобы узнать, какие клиенты затронуты, выберите вкладки Приложения, Виртуальные или Системы. • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.
8 Убедитесь, что пулы хранения доступны для резервного копирования данных клиента.	1. Если в области Хранение и доступность данных указаны проблемы, щелкните по Пулы, чтобы ознакомиться со сведениями: ◦ Если показано состояние Критическое ⊗, это указывает на то, что в пуле хранения недостаточно доступного пространства или его состояние доступа - Недоступно. Внимание: Если состояние критическое, то изучите причину: ▪ Если скорость дедупликации данных в пуле хранения значительно снижается, то это может указывать на атаку программы-вымогателя. Во время атаки программы-вымогателя данные шифруются и не могут дедуплицироваться. Чтобы проверить скорость дедупликации данных, в таблице Пулы хранения проверьте значение в столбце Процент экономии. ▪ Если пул хранения неожиданно становится использован 100%, то это может указывать на атаку программы-	Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по Сведения.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
	вымогателя. Для проверки использования просмотрите значение в столбце Использованная емкость. Наведите мышь на значения, чтобы увидеть процент использованного и свободного пространства. ○ Если показано состояние Предупреждение ⚠, в пуле хранения заканчивается пространство или его состояние доступа - Только чтение. 2. Чтобы увидеть и используемое, свободное и общее пространство для выбранного пула хранения, установите указатель мыши над записями в столбце Использованная емкость.	
9 Убедитесь, что устройства хранения доступны для операций резервного копирования.	В области Хранение и доступность данных, в разделе Тома под столбцами емкости проверьте состояние, показанное рядом с элементом Устройства. Если для любого устройства показано состояние Критическое ✕ или Предупреждение ⚠, исследуйте проблему. Чтобы просмотреть сведения, щелкните по Устройства.	Дисковые устройства могут находиться в критическом состоянии или в состоянии предупреждения по следующим причинам: • Для классов устройств DISK тома могут быть отключены или находиться в состоянии 'только для чтения'. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние томов. • Для классов устройств FILE, которые не используются совместно, могут быть отключены каталоги. Кроме того, для выделения чистых томов может оказаться недостаточно свободного пространства. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние каталогов. • Для классов устройств FILE, которые используются совместно, могут быть недоступны накопители. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. В других столбцах таблицы Дисковые устройства показано состояние накопителей и путей.

Контрольный список периодического мониторинга

Чтобы убедиться, что ваше решение IBM Spectrum Protect работает правильно, выполните задачи в периодическом контрольном списке мониторинга. Запланируйте периодические задачи достаточно часто, чтобы вы могли обнаружить потенциальные неполадки, прежде чем они вызовут проблемы.

Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров  и щелкните по Построитель команд.

Табл. 1. Задачи периодического мониторинга

Задача	**Основные процедуры**	**Дополнительные процедуры и устранение ошибок**
Отслеживайте производительность системы.	Определите, сколько времени требуется для операций резервного копирования клиента: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Найдите сервер, связанный с клиентом. 2. Щелкните по Серверы. Выберите сервер и щелкните по Сведения. 3. Чтобы увидеть продолжительность выполненных задач за последние 24 часа, щелкните по Выполненные задачи. 4. Чтобы увидеть продолжительность задач, выполненных более 24 часов тому назад, используйте команду QUERY ACTLOG. Следуйте инструкциям в разделе . 5. Если длительность операций резервного копирования клиента увеличивается при неясных причинах, исследуйте причину. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете диагностировать ошибки, влияющие на производительность, для клиента резервного копирования и архивирования, выполнив следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. 2. Выберите клиент резервного копирования и архивирования и щелкните по Сведения. 3. Чтобы получить журналы клиентов, щелкните по Диагностика.	Инструкции по сокращению времени, которое затрачивает клиент на резервное копирование данных на сервер, смотрите в разделе Устранение общих проблем, связанных с производительностью клиента. Ищите узкие места с точки зрения производительности. Инструкции смотрите в разделе Выявление узких мест производительности. Информацию о выявлении и устранении других проблем, отрицательно влияющих на производительность, смотрите в разделе Производительность.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите экономию дисков, обеспечиваемую дедупликацией данных.	1. Щелкните на странице Обзор в компоненте Центр операций по Пулы. 2. Выберите пул щелкните по Быстрый обзор. 3. В области Дедупликация данных смотрите сохраненную строку Пространство.	При расширенном мониторинге, чтобы получить подробную статистику процесса дедупликации данных для определенного пула хранения контейнеров каталогов или облачного пула хранения каталогов, выполните следующие шаги: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Получите статистический отчет, введя команду GENERATE DEDUPSTATS. Следуйте инструкциям в разделе GENERATE DEDUPSTATS (Сгенерировать статистику дедупликации данных для пула хранения каталога-контейнера). 3. Просмотрите статистический отчет, введя команду QUERY DEDUPSTATS. Следуйте инструкциям в разделе QUERY DEDUPSTATS (Запросить статистику дедупликации данных).

Убедитесь, что текущие файлы резервных копий для конфигурации устройств и информации о хронологии томов сохранены.	Получите доступ к расположениям хранения, чтобы убедиться, что файлы доступны. Предпочтительный метод заключается в том, чтобы сохранять файлы резервных копий в двум расположениях.
	Чтобы найти файлы хронологии томов и файлы конфигурации устройств, выполните следующие шаги:
	1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
	2. Чтобы найти файлы хронологии томов и конфигурации устройств, введите следующие команды:
	`query option volhistory`
	`query option devconfig`
	3. В выходной информации проверьте столбец Параметр опции, чтобы найти расположения файлов.
	Если произойдет бедствие, для восстановления базы данных сервера потребуется как файл хронологии томов, так и файл конфигурации устройств.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите, доступно ли достаточно пространства для файловой системы каталога экземпляра.	Убедитесь, что в файловой системе каталога экземпляра доступно, как минимум, 20% свободного пространства. Выполните действие, подходящее для вашей операционной системы: •  Операционные системы AIX Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -g` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Linux Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -h` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Windows В проводнике Windows щелкните правой кнопкой мыши по файловой системе и выберите Свойства. Проверьте информацию о емкости. Предпочтительное расположение каталога экземпляра зависит от операционной системы, в которой установлен сервер: •  Операционные системы AIX  Операционные системы Linux /home/tsminst1/tsminst1  Операционные системы Windows C:\tsminst1 Совет: Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Выявите неожиданную активность клиента.	Чтобы отслеживать операции клиента и определить, не превышает ли объем данных для томов ожидаемый объем, выполните следующие шаги: 1. На странице Обзор в компоненте Центр операций щелкните по области Клиенты. 2. Чтобы увидеть операции за посредние две недели, дважды щелкните по любому клиенту. 3. Чтобы узнать число байт, отправленных клиенту, щелкните по вкладке Свойства. 4. В области Последний сеанс проверьте строку Отправлено клиенту.	Когда вы дважды щелкнете по клиенту в таблице Клиенты, в области Операции за 2 недели будет показан объем данных, которые клиент каждый день отправлял на сервер. Регулярно проверяйте SQL-таблицу сводной информации о деятельности, содержащую статистические данные о клиентских сеансах. Чтобы сравнить текущие операции с предыдущими, воспользуйтесь оператором SQL SELECT. Если уровень операций существенно отличается от предыдущего, то это может указывать на атаку программы-вымогателя. Регулярно проверяйте журнал операций. Найдите сообщения ANE, указывающие, для скольких файлов созданы резервные копии и выполнена инспекция. Сравните текущие данные о скорости дедупликации с прежней скоростью. Если в созданной резервной копии необычно много файлов или уровень дедупликации данных неожиданно спадает до 0, то это может указывать на атаку программы-вымогателя

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте рост пула хранения с течением времени.	1. На странице Обзор в компоненте Центр операций щелкните по области Пулы. 2. Чтобы увидеть емкость, используемую за последние две недели, выберите пул и щелкните по Сведения.	Советы: • Чтобы задать период времени, который должен пройти, прежде чем из пула хранения каталогов-контейнеров или пула хранения облачных контейнеров будут удалены все дедуплицированные экстенты, после того как на них не появлялось никаких ссылок в перечне, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. 3. Задайте длительность в поле `Период задержки для повторного использования контейнера`. • Чтобы определить производительность дедупликации данных для пулов хранения каталогов-контейнеров и облачных контейнеров, используйте команду GENERATE DEDUPSTATS. • Чтобы просмотреть статистику дедупликации данных для пула хранения, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. Либо используйте команду QUERY EXTENTUPDATES, чтобы увидеть информацию об обновлениях экстентов данных в пулах хранения каталогов-контейнеров или облачных контейнеров. Выходная информация команды может помочь вам определить, на какие экстенты данных уже нет ссылок и какие из них подлежат удалению из системы. В выходной информации смотрите, какое число экстентов данных подлежит удалению из системы. Этот показатель напрямую коррелируется с объемом свободного пространства, которое будет доступно в пуле хранения контейнера. • Чтобы увидеть объем физического пространства, занятого файловым пространством после удаления экономии за счет дедупликации данных, используйте команду select * from occupancy. В выходной информации команды будет содержаться значение LOGICAL_MB. LOGICAL_MB - это объем, используемый этим файловым пространством.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Оцените временные характеристики расписаний клиента. Убедитесь, что начальное и конечное время расписаний клиентов соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Клиенты > Расписания. В таблице Расписания в столбце Запуск показано сконфигурированное время запуска для запланированной операции. Чтобы увидеть, когда была запущена самая последняя операция, установите указатель мыши на значок часов.	Совет: Если операция клиента выполняется дольше, чем ожидается, вы можете получить сообщение с предупреждением. Сделайте следующее: 1. На странице обзора в компоненте Центр операций установите указатель мыши на Клиенты и щелкните по Расписания. 2. Выберите расписание и щелкните по Сведения. 3. Просмотрите сведения о расписании, щелкнув по синей стрелке рядом со строкой. 4. В поле Оповещение среды выполнения задайте время, когда будет выдано сообщение с предупреждением, если запланированная операция не будет выполнена. 5. Щелкните по Сохранить.
Оцените временные характеристики задач по обслуживанию. Убедитесь, что начальное и конечное время задач по обслуживанию соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Серверы > Обслуживание. В таблице Обслуживание проверьте информацию в столбце Время последнего выполнения. Чтобы увидеть, когда была запущена самая последняя задача по обслуживанию, установите указатель мыши на значок часов.	Совет: Если задача по обслуживанию выполняется слишком долго, измените начальное время или максимальное время выполнения. Сделайте следующее: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров  и щелкните по Построитель команд. 2. Чтобы изменить время запуска или максимальное время выполнения задачи, введите команду UPDATE SCHEDULE. Инструкции смотрите в разделе UPDATE SCHEDULE (Изменить запланированное задание клиента).

Ссылки, связанные с данной:

QUERY ACTLOG (Запросить информацию журнала операций)

UPDATE STGPOOL (обновить пул хранения)

QUERY EXTENTUPDATES (Запросить обновленные экстенты данных)

Проверка на соответствие лицензии

Убедитесь, что ваше решение IBM Spectrum Protect соответствует положениям вашего лицензионного соглашения. Регулярно производя мониторинг решения, можно отслеживать тенденции роста данных или использование единиц мощности процессора (processor value unit, PVU). Используйте эту информацию, чтобы спланировать будущее приобретение лицензий.

Об этой задаче

Метод, который вы используете, чтобы убедиться, что ваше решение соответствует условиям лицензии, зависит от положений вашего лицензионного соглашения IBM Spectrum Protect.

Фронтальное лицензирование мощности

Фронтальная модель определяет требования к лицензии на основе объема первичных данных, о которых клиентами было сообщено, что для них создавались резервные копии. К клиентам относятся приложения, виртуальные машины и компьютеры.

Внутреннее лицензирование мощности
Внутренняя модель определяет требования к лицензии на основе числа терабайт данных, которые хранятся в первичных пулах хранения и репозиториях.
Советы:

- Чтобы обеспечить точность оценки фронтальной и внутренней емкости, установите новейшую версию программы клиента на каждом клиентском узле.
- Информация о фронтальной и внутренней емкости в Центр операций предназначена только для планирования и оценки.

Лицензирование PVU
Модель PVU основана на использовании PVU серверными устройствами.
Важное замечание: Расчеты PVU, выполняемые IBM Spectrum Protect, считаются оценочными и не имеют юридической силы. Информация о лицензировании PVU, сообщенная продуктом IBM Spectrum Protect, не рассматривается как допустимая замена для IBM® License Metric Tool.

Самую последнюю информацию о моделях лицензирования смотрите в информации о продукте и лицензии на веб-сайте семейства продуктов IBM Spectrum Protect. Если у вас возникнут вопросы или замечания, касающиеся требований по лицензированию, обращайтесь к вашему поставщику программы IBM Spectrum Protect.

Процедура

Чтобы отследить соответствие лицензии, выполните шаги, соответствующие положениям вашего лицензионного соглашения.
Совет: Центр операций обеспечивает электронный отчет, в котором просуммировано использование фронтальной и внутренней емкости. Отчеты можно автоматически регулярно отправлять одному или нескольким получателям. Чтобы сконфигурировать электронные отчеты и управлять ими, щелкните по Отчеты в строке меню Центр операций.

Опция	Описание
Фронтальная модель	a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. На странице Фронтальное использование показана оценка фронтальной емкости. b. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости. c. Чтобы оценить емкость для клиентов, которые не сообщают об использовании емкости, перейдите на следующий FTP-сайт, где представлены инструменты измерения и инструкции: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Чтобы изменить фронтальную емкость в соответствии со сценарием, выполните инструкции в самом последнем доступном руководстве по лицензированию. d. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария. e. Убедитесь, что оценка емкости соответствует вашему лицензионному соглашению.

Опция	Описание
Внутренняя модель	Ограничение: Если исходный и целевой серверы репликации не используют одни и те же параметры политики, вы не сможете использовать Центр операций для мониторинга использования внутренней емкости для реплицируемых клиентов. Информацию о том, как оценить использование емкости для этих клиентов, смотрите в следующей публикации technote 1656476. a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. b. Щелкните по вкладке Внутренний. c. Проверьте, соответствует ли оценка объема данных вашему лицензионному соглашению.
Модель PVU	Иформацию о том, как оценить соответствие условиям лицензирования PVU, смотрите в разделе Оценка соответствия модели лицензирования PVU.

Состояние системы отслеживания с использованием отчетов по электронной почте

Настройте компонент Центр операций, чтобы сгенерировать отчеты по электронной почте, в которых суммируется состояние системы. Вы можете сконфигурировать соединение с почтовым сервером, изменить параметры отчета и (необязательно) создать пользовательские отчеты.

Прежде чем начать

Прежде чем настраивать отчеты по электронной почте, убедитесь, что выполнены следующие требования:

- Доступен хост-сервер Simple Mail Transfer Protocol (SMTP) для отправки и получения отчетов по электронной почте. Сервер SMTP должен быть сконфигурирован как открытый почтовый ретранслятор. Вы также должны убедиться, что у сервера IBM Spectrum Protect, который отправляет сообщения электронной почты, есть доступ к серверу SMTP. Если центр операций установлен на отдельном компьютере, этому компьютеру не требуется доступ к серверу SMTP.
- Чтобы задавать отчеты по электронной почте, нужно иметь системные полномочия для сервера.
- Чтобы задать получателей, можно ввести один или несколько адресов электронной почты или ID администраторов. Если вы собираетесь ввести ID администратора, ID должен быть зарегистрирован на хаб-сервере и с ним должен быть связан адрес электронной почты. Чтобы задать адрес электронной почты для администратора, используйте параметр EMAILADDRESS в команде UPDATE ADMIN.

Об этой задаче

Вы можете сконфигурировать Центр операций для отправки отчета об общих операциях, отчета о соответствии лицензии, а также одного или нескольких пользовательских отчетов. Вы создаете пользовательские отчеты, выбирая шаблоны из набора обычно используемых шаблонов отчетов или вводя операторы SQL SELECT, чтобы запросить информацию на управляемых серверах.

Процедура

Чтобы настроить электронные отчеты и управлять ими, сделайте следующее:

1. В строке меню компонента Центр операций выберите Отчеты.
2. Если соединение с сервером электронной почты еще не сконфигурировано, щелкните по Сконфигурировать почтовый сервер и заполните поля. После того как вы сконфигурируете почтовый сервер, будут включены отчет об общих операциях и отчет о соответствии лицензии.
3. Чтобы изменить параметры отчета, выберите отчет, щелкните по Сведения и обновите форму.
4. Необязательно: Чтобы добавить пользовательский отчет, щелкните по + Отчет и заполните поля.
   Совет: Чтобы сразу же запустить и отправить отчет, выберите отчет и нажмите на Отправить.

Результаты

Разрешенные отчеты будут отправлены в соответствии с заданными параметрами.

Ссылки, связанные с данной:

UPDATE ADMIN (обновление администратора)

Управление операциями для дискового решения с одной площадкой

Используйте эту информацию для управления операциями при дисковом решении для одной площадки с IBM Spectrum Protect, включающим в себя сервер и использующим дедупликацию данных для одной площадки.

- Управление Центром операций
  Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.
- Защита приложений, виртуальных машин и компьютеров
  Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.
- Управление хранилищем данных
  Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.
- Защита сервера IBM Spectrum Protect
  Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.
- Остановка и запуск сервера
  Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.
- Планирование обновления сервера
  Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.
- Подготовка к отключению или обновлению системы
  Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.
- Реализация плана аварийного восстановления
  Примените стратегию аварийного восстановления, чтобы восстановить приложения, если произойдет авария, и обеспечить высокую доступность сервера.
- Восстановление после перебоев в работе системы
  В случае дисковых решений IBM Spectrum Protect с одной площадкой можно только восстановить перечень на локальном компьютере и восстановить базу данных, чтобы защитить ваши данные.

Управление Центром операций

Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.

- Добавление и удаление подчиненных серверов
  В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.
- Запуск и остановка веб-сервера
  Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.
- Перезапуск мастера начального конфигурирования
  Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.
- Изменение хаб-сервера
  Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.

- Восстановление конфигурации до предварительно сконфигурированного состояния
  При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Добавление и удаление подчиненных серверов

В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

Об этой задаче

Подчиненные серверы отправляют оповещения и информацию о состоянии хаб-серверу. Центр операций содержит консолидированное представление оповещений и информации о состоянии для хаб-сервера и всех подчиненных серверов.

- Добавление подчиненного сервера
  После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.
- Удаление подчиненного сервера
  Можно удалить подчиненный сервер из Центра операций.

Добавление подчиненного сервера

После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.

Прежде чем начать

Связь между подчиненным сервером и хаб-сервером должна быть защищена с использованием протокола Transport Layer Security (TLS). Для защиты связи добавьте сертификат подчиненного сервера в файл доверенных сертификатов хаб-сервера.

Процедура

1. Щелкните в панели меню Центр операций по Серверы. Откроется страница Серверы.

   В таблице на странице Серверы состоянием сервера может быть "Не отслеживается" Это состояние означает, что хотя администратор и определил этот сервер на хаб-сервере при помощи команды DEFINE SERVER, этот сервер еще не сконфигурирован в качестве подчиненного сервера.

2. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по Отслеживать подчиненный.
   - Если сервера, который вы хотите добавить, нет в таблице, а защищенная связь SSL/TLS не требуется, то щелкните по + Подчиненный в панели меню таблицы.
3. Задайте нужную информацию и выполните действия в мастере конфигурирования подчиненных серверов.
   Совет: Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как подчиненный сервер.

Удаление подчиненного сервера

Можно удалить подчиненный сервер из Центра операций.

Об этой задаче

Вам может потребоваться удалить подчиненный сервер, например, в следующих ситуациях:

- Вы хотите переместить подчиненный сервер с одного хаб-сервера на другой.
- Подчиненный сервер больше не нужен.

Процедура

Чтобы удалить подчиненный сервер из группы серверов, которая управляется хаб-сервером, сделайте следующее:

1. В командной строке IBM Spectrum Protect введите следующую команду для хаб-сервера:

   ```
   QUERY MONITORSETTINGS
   ```

2. Скопируйте в выходных результатах команды имя, указанное в поле Отслеживаемые группы.
3. Введите на хаб-сервере следующую команду, где *имя_группы* - это имя отслеживаемой группы, а *имя_члена* - это имя подчиненного сервера.

   ```
   DELETE GRPMEMBER имя_группы имя_члена
   ```

4. Необязательно: Если вы хотите переместить подчиненный сервер с одного хаб-сервера на другой, **не** выполняйте этот шаг. В ином случае можно запретить оповещения и мониторинг для подчиненного сервера, введя на подчиненном сервере следующие команды:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Необязательно: Если определение подчиненного сервера используется в других целях, например, для конфигурирования предприятия, маршрутизации команд, хранения виртуальных томов или управления библиотекой, **не** выполняйте этот шаг. В противном случае можно удалить определение подчиненного сервера на хаб-сервере, введя на хаб-сервере следующую команду:

   ```
   DELETE SERVER имя_подчиненного_сервера
   ```

   Совет: Если определение сервера удаляется сразу же после удаления сервера из отслеживаемой группы, информация о состоянии сервера может остаться в центре операций на неопределенно долгое время.

   Чтобы избежать этой проблемы, перед удалением определения сервера дождитесь, когда пройдет интервал сбора состояния. Интервал сбора данных состояния показан на странице Параметры в центре операций.

Запуск и остановка веб-сервера

Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.

Процедура

1. Остановите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./stopserver.sh
     ```

   - Операционные системы LinuxВведите следующую команду:

     ```
     service opscenter.rc stop
     ```

   - Операционные системы WindowsВ окне Службы остановите службу Центр операций IBM Spectrum Protect.
2. Запустите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./startserver.sh
     ```

   - Операционные системы LinuxВведите следующие команды:

     Запустите сервер:

     ```
     service opscenter.rc start
     ```

     Перезапустите сервер:

     ```
     service opscenter.rc restart
     ```

Определите, работает ли сервер:

```
service opscenter.rc status
```

- Операционные системы WindowsВ окне Службы запустите службу Центр операций IBM Spectrum Protect.

Перезапуск мастера начального конфигурирования

Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.

Прежде чем начать

Чтобы изменить следующие параметры, используйте страницу Параметры в Центр операций вместо перезапуска мастера начального конфигурирования:

- Периодичность обновления данных
- Интервал времени, в течение которого предупреждение активно, неактивно или закрывается
- Условия, обозначающие риск для клиентов

Центр операций помогает включить дополнительную информацию о том, как изменить эти параметры.

Об этой задаче

Для перезапуска мастера начального конфигурирования необходимо удалить файл свойств с информацией о соединении с хаб-сервером. Однако никакие настройки оповещений, мониторинга, состояния 'Под угрозой' или среды для нескольких серверов, заданные для хаб-сервера, не удаляются. Эти настройки используются как настройки мастера конфигурирования по умолчанию при его перезапуске.

Процедура

1. Остановите веб-сервер Центр операций.
2. На компьютере с установленным продуктом Центр операций перейдите в следующий каталог, где *каталог_установки* представляет собой каталог, в котором установлен продукт Центр операций:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer

   Например:
   - Операционные системы AIXОперационные системы Linux/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windowsc:\Program Files\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Удалите из каталога guiServer файл serverConnection.properties.
4. Запустите веб-сервер Центра операций.
5. Откройте Центр операций.
6. Переконфигурируйте Центр операций при помощи мастера конфигурирования. Задайте новый пароль для ID администратора мониторинга.
7. На каждом из подчиненных серверов, ранее связанных с хаб-сервером, измените пароль для ID администратора мониторинга, введя следующую команду в интерфейсе командной строки IBM Spectrum Protect:

   ```
   UPDATE ADMIN  IBM-OC-имя_хаб-сервера новый_пароль
   ```

   Ограничение: Не изменяйте никакие другие параметры для этого ID администратора. После того, как задан начальный пароль, он автоматически управляется Центр операций.

Изменение хаб-сервера

Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.

Процедура

1. Перезапустите мастер начального конфигурирования Центр операций. При выполнении этой процедуры вы удаляете соединение хаб-сервера.
2. При помощи мастера сконфигурируйте Центр операций для соединения с новым хаб-сервером.

Задачи, связанные с данной:
Перезапуск мастера начального конфигурирования

Восстановление конфигурации до предварительно сконфигурированного состояния

При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Процедура

Чтобы восстановить конфигурацию, выполните следующие шаги:

1. Остановите веб-сервер Центр операций.
2. Деконфигурируйте хаб-сервер, выполнив следующие действия:
   a. Введите на хаб-сервере следующие команды:

   ```
   SET MONITORINGADMIN ""
   SET MONITOREDSERVERGROUP ""
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   REMOVE ADMIN IBM-OC-имя_хаб-сервера
   ```

   Совет: `IBM-OC-`*`имя_хаб-сервера`* - это ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Переустановите пароль для хаб-сервера, введя на хаб-сервере следующую команду:

   ```
   SET SERVERPASSWORD ""
   ```

   Внимание: Не выполняйте этот шаг, если хаб-сервер сконфигурирован с другими серверами для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.
3. Отмените конфигурацию всех подчиненных серверов, выполнив следующие шаги:
   a. Чтобы определить, остаются ли какие-либо подчиненные серверы как члены группы серверов, введите на хаб-сервере следующую команду:

   ```
   QUERY SERVERGROUP IBM-OC-имя_хаб-сервера
   ```

   Совет: `IBM-OC-`*`имя_хаб-сервера`* - это имя отслеживаемой группы серверов, которая была автоматически создана при конфигурировании первого подчиненного сервера. Это имя группы серверов - это также ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Чтобы удалить из группы серверов подчиненные серверы, введите на хаб-сервере следующую команду для каждого подчиненного сервера:

   ```
   DELETE GRPMEMBER IBM-OC-имя_хаб-сервера имя_подчиненного_сервера
   ```

   c. После удаления всех подчиненных серверов из группы серверов введите следующую команду на хаб-сервере:

   ```
   DELETE SERVERGROUP IBM-OC-имя_хаб-сервера
   SET MONITOREDSERVERGROUP ""
   ```

   d. Введите на каждом подчиненном сервере следующую команду:

   ```
   REMOVE ADMIN IBM-OC-имя_хаб-сервера
   SETOPT PUSHSTATUS NO
   SET ALERTMONITOR OFF
   SET STATUSMONITOR OFF
   ```

   e. Удалите на каждом из подчиненных серверов определение хаб-сервера, введя на серверах следующую команду:

   ```
   DELETE SERVER имя_хаб_сервера
   ```

Внимание: Не выполняйте этот шаг, если данное определение используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.

f. Удалите на хаб-сервере определение каждого из подчиненных серверов, введя следующую команду:

```
DELETE SERVER имя_подчиненного_сервера
```

Внимание: Не выполняйте этот шаг, если данное определение сервера используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.

4. Восстановите параметры по умолчанию для каждого сервера, введя следующие команды:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Перезапустите мастер начального конфигурирования Центр операций.

Задачи, связанные с данной:
Перезапуск мастера начального конфигурирования
Запуск и остановка веб-сервера

Защита приложений, виртуальных машин и компьютеров

Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.

- Добавление клиентов
  После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.
- Управление операциями клиентов
  Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.
- Управление обновлениями клиентов
  Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).
- Списание клиентского узла
  Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).
- Деактивация данных для высвобождения пространства хранения
  В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Добавление клиентов

После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.

Об этой задаче

Процедура описывает базовые шаги по добавлению клиента. Более конкретные инструкции по конфигурированию клиентов смотрите в документации по продукту, который вы установили на клиентском узле. У вас могут быть следующие

типы клиентских узлов:

Клиентские узлы приложений
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Системные клиентские узлы
: К системным клиентским узлам относятся рабочие станции, файл-серверы сетевого хранилища данных (NAS) и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Процедура

Чтобы добавить клиент, сделайте следующее:

1. Выберите программу, которую нужно установить на клиентском узле, и спланируйте установку. Следуйте инструкциям в разделе Выбор программного обеспечения клиента и планирование установки.
2. Укажите, как следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе Как задать роли для резервного копирования и архивирования данных клиента.
3. Укажите, когда следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе Планирование операций резервного копирования и архивирования.
4. Чтобы позволить клиенту соединяться с сервером, зарегистрируйте клиент. Следуйте инструкциям в разделе Регистрация клиентов.
5. Чтобы начать защищать клиентский узел, установите и сконфигурируйте выбранную программу на клиентском узле. Следуйте инструкциям в разделе Установка и настройка клиентов.

Выбор программного обеспечения клиента и планирование установки

Для разных типов данных требуются разные типы защиты. Определите, какой тип данных вам нужно защищать, и выберите соответствующую программу.

Об этой задаче

Предпочтительная практика заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить демон приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, вы должны следовать инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Процедура

В зависимости от ваших целей выберите продукты, которые нужно установить, и ознакомьтесь с инструкциями по установке.
Совет: Если вы установите программу-клиент сейчас, вы, прежде чем сможете использовать клиент, также должны будете выполнить задачи по конфигурированию клиента, описанные в разделе Установка и настройка клиентов.

Цель	Продукт и описание	Инструкции по установке

Цель	Продукт и описание	Инструкции по установке
Защитить файл-сервер или рабочую станцию	Клиент резервного копирования и архивирования производит резервное копирование и архивирование файлов и каталогов с файл-серверов и рабочих станций в хранилище. Вы также можете восстанавливать и получать версии резервных копий и архивные копии файлов.	• Требования клиента резервного копирования и архивирования • Установить клиентов резервного копирования и архивирования UNIX и Linux • Первая установка клиента Windows
Защитить приложения с использованием резервного копирования снимков и возможностей восстановления	IBM Spectrum Protect Snapshot защищает данные с использованием интегрированного резервного копирования снимков и возможностей восстановления с учетом информации о приложениях. Вы можете защитить данные, которые хранятся в приложениях IBM программное обеспечение баз данных DB2 и SAP, Oracle, Microsoft Exchange и Microsoft SQL Server.	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
Защитить приложение электронной почты на сервере IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов IBM Domino.	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0)
Защитить приложение электронной почты на сервере Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов Microsoft Exchange.	Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Защитить базу данных IBM DB2	Интерфейс прикладного программирования (API) можно использовать для резервного копирования данных DB2 на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных IBM Informix	API клиента резервного копирования и архивирования можно использовать для резервного копирования данных Informix на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных Microsoft SQL	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server защищает данные Microsoft SQL.	Установка Data Protection for SQL Server в ядре сервера Windows
Защитить базу данных Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle защищает данные Oracle.	Установка Data Protection for Oracle
Защитить среду SAP	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP обеспечивает защиту, настроенную для сред SAP. Продукт предназначен для того, чтобы повышать доступность серверов базы данных SAP и сокращать рабочую нагрузку администрирования.	• Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

Цель	Продукт и описание	Инструкции по установке
Защитить виртуальную машину	IBM Spectrum Protect for Virtual Environments обеспечивает защиту, настроенную для виртуальных сред Microsoft Hyper-V и VMware. IBM Spectrum Protect for Virtual Environments можно использовать для создания постоянных инкрементных резервных копий, хранящихся на централизованном сервере, создания политик резервного копирования и восстановления виртуальных машин или отдельных файлов. Либо используйте клиент резервного копирования и архивирования, чтобы производить резервное копирование и восстановление полной виртуальной машины VMware или Microsoft Hyper-V. Можно также производить резервное копирование и восстановление файлов или каталогов с виртуальной машины VMware.	• Установка Data Protection for Microsoft Hyper-V • Установка и обновление Data Protection for VMware • Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)

Совет: Чтобы использовать клиент для управления пространством, можно установить IBM Spectrum Protect for Space Management или IBM Spectrum Protect HSM for Windows.

Как задать роли для резервного копирования и архивирования данных клиента

Прежде чем вы добавите клиент, убедитесь, что соответствующие правила определены для поддержки и архивирования клиентских данных. В ходе процесса регистрации клиента вы назначается клиентский узел в домен политики, в котором есть правила, управляющие тем, как и когда производится сохранение данных клиента.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с политиками, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Планирование операций резервного копирования и архивирования.
- Если вы не знакомы с политиками, то выполните шаги в этой процедуре.

Об этой задаче

Политики влияют на то, какой объем данных хранится в течение долгого времени и сколько времени данные сохраняются и будут доступны клиентам для восстановления. Для достижения целей для защиты данных можно обновить политику по умолчанию и создать собственные политики. Политика включает следующие правила:

- Как и когда производится резервное копирование и архивирование файлов в серверное хранилище.
- Число копий файла и время хранения копий в серверном хранилище.

В ходе процесса регистрации клиента вы назначается клиент в *домен политики*. Политика для отдельного клиента определяется правилами в домене политики, который назначен для клиента. В домене политики действующие правила находятся в активном *наборе политик*.

Когда клиент копирует или архивирует файл, файл привязывается к классу управления в активном наборе политик домена политики. *Класс управления* - это ключевой набор правил для управления данными клиента. Операции резервного копирования и архивирования на клиенте используют настройки в классе управления по умолчанию домена политики, если вы далее не настраиваете политику. Политику можно настроить, задав больше классов управления и назначив их использование через опции клиента.

Опции клиента можно задать в локальном, доступном для изменения файле в системе клиента и в наборе опций клиента на сервере. Опции в наборе опций клиента на сервере могут переопределять локальный файл опций клиента или могут добавлять в него опции.

Процедура

1. Ознакомьтесь с политиками, сконфигурированными для вашего решения - следуйте инструкциям в разделе Просмотр политик.
2. Если необходимо внести незначительные изменения для соответствия требованиям хранения данных, следуйте инструкциям в разделе Изменение политик.
3. Необязательно: Если вам нужно создать домены политики или внести расширенные изменения в политики, чтобы выполнить требования к хранению данных, смотрите раздел Настройка политик.

Просмотр политик

Просмотрите политики, чтобы определить, не нужно ли их изменить в соответствии с вашими требованиями.

Процедура

1. Чтобы просмотреть активный наборов политик для домена политики, сделайте следующее:
   a. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
   b. На странице Сводка для домена политики щелкните по вкладке Наборы политики.
   Совет: Чтобы облегчить возможность восстановления данных после атаки программы-вымогателя, следуйте инструкциям ниже:
      - Убедитесь, что значение в столбце Резервные копии - это минимум 2. Предпочтительное значение - 3, 4 или более.
      - Убедитесь, что значение в столбце Сохранять дополнительные резервные копии - это минимум 14 дней. Предпочтительное значение равно 30 или более дням.
      - Убедитесь, что значение в столбце Сохранять архивы - это минимум 30 дней.

   Если программа IBM Spectrum Protect for Space Management установлена на клиенте, то убедитесь, что создана резервная копия данных, перед тем как перемещать данные. В команде DEFINE MGMTCLASS или UPDATE MGMTCLASS задайте MIGREQUIRESBKUP=YES. Далее следуйте руководящим подсказкам.
2. Для просмотра бездействующих наборов политики для домена политики сделайте следующее:
   a. На странице Наборы политик щелкните по Конфигурировать. Теперь можно просмотреть и изменить неактивные наборы политики.
   b. Прокрутите неактивные наборы политик, используя стрелки Вперед и Назад. При просмотре неактивного набора политики параметры, которые отличают этот неактивный набор политик от активного набора политик, будут выделены.
   c. Щелкните по переключателю Конфигурировать. Теперь наборы политик больше нельзя изменять.

Изменение политик

Чтобы изменить правила, применимые к домену политики, измените активный набор политик для домена политики. Можно также активировать для домена другой набор политик.

Прежде чем начать

Изменения политики могут повлиять на хранение данных. Убедитесь, чтобы вы продолжаете резервное копирование данных, имеющих существенное значение для вашей организации, чтобы можно было восстановить эти данные, если произойдет бедствие. Также убедитесь, что в вашей системе достаточно пространства хранения для запланированных операций резервного копирования.

Об этой задаче

Вы изменяете набор политик, изменяя один или несколько классов управления в наборе политик. Если вы измените активный набор политик, изменения не будут доступны клиентам, пока вы не активируете повторно набор политик. Чтобы сделать измененный набор политик доступным клиентам, активируйте набор политик.

Хотя для домена политики можно задать несколько наборов политик, активным может быть только один набор политик. При активации другого набора политики он заменяет активный в данный момент набор политик.

Предпочтительный опыт определения политик описан в разделе Настройка политик.

Процедура

1. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики.

   На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.

3. Щелкните по переключателю Конфигурировать. Набор политик доступен для изменения.
4. Необязательно: Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
5. Измените набор политик, выполнив любое из следующих действий:

Опция	Описание
Добавьте класс управления	a. В таблице Наборы политик щелкните по +Класс управления. b. Чтобы задать правила для резервного копирования и архивирования данных, заполните поля в окне Добавить класс управления. c. Чтобы сделать класс управления классом управления по умолчанию, включите переключатель Сделать значением по умолчанию. d. Щелкните по Добавить.
Удалите класс управления	В столбце Класс управления щелкните по -. Совет: Чтобы удалить класс управления по умолчанию, нужно сначала назначить другой класс управления классом управления по умолчанию.
Сделать класс управления классом управления по умолчанию	Щелкните по радиокнопке в столбце Значение по умолчанию для класса управления. Совет: Класс управления по умолчанию управляет файлами клиента, если для файла не назначен другой класс управления или если класс управления файла не подходит для управления файлом. Чтобы убедиться в том, что клиенты всегда могут производить резервное копирование и архивирование файлов, выберите класс управления по умолчанию и для резервного копирования, и для архивирования файлов.
Изменить класс управления	Чтобы изменить свойства класса управления, обновите поля в таблице.

6. Щелкните по Сохранить.
   Внимание: При активации нового набора политик можно потерять данные. Данные, защищенные в соответствии с одним набором политик, могут оказаться незащищенными с точки зрения другого набора политик. Поэтому, прежде чем активировать набор политик, убедитесь, что разница между предыдущим набором политик и новым набором политик не вызовет потерю данных.
7. Выберите Активировать. Будет показана сводка различий между активным набором политик и новым набором политик. Убедитесь, что изменения в новом наборе политики совместимы с вашими требованиями к хранению данных; для этого выполните следующие шаги:
   a. Проверьте различия между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном наборе политик, будут связаны с классами управления с теми же именами в новом наборе политик.
   b. Укажите в активном наборе политики классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут управляться классом управления по умолчанию в новом наборе политик.
   c. Если изменения, которые должны быть реализованы набором политики, являются допустимыми, выберите переключатель Я понимаю, что эти обновления могут вызвать потерю данных и щелкните по Активировать.

Планирование операций резервного копирования и архивирования

Прежде чем зарегистрировать новый клиент на сервере, убедитесь, что существует расписание, позволяющее указать, когда выполняются операции резервного копирования и архивирования. В процессе регистрации можно назначить расписание клиенту.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с расписаниями, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Регистрация клиентов.
- Если вы не знакомы с расписаниями или расписания нужно изменить, выполните шаги в этой процедуре.

Об этой задаче

Как правило, операции резервного копирования для всех клиентов должны выполняться ежедневно. Спланируйте рабочую нагрузку клиента и сервера, чтобы обеспечить наивысшую производительность для вашей среды хранения. Чтобы избежать перекрывания операций клиента и сервера, рассмотрите возможность запланировать выполнение операций резервного копирования и архивирования клиента по ночам. Если операции клиента и сервера будут перекрываться или для их обработки не выделят достаточно времени и ресурсов, то вы можете столкнуться со снижением производительности системы, неудачным завершением операций и другими проблемами.

Процедура

1. Проверьте доступные расписания, установив указатель мыши на Клиенты в строке меню Центр операций. Щелкните по Расписания.
2. Необязательно: Измените или создайте расписание, выполнив следующие шаги:

Опция	Описание
Изменение расписания	a. В представлении Расписания выберите расписание и щелкните по Сведения. b. На странице Сведения о расписании просмотрите сведения, щелкнув по синим стрелкам в начале строк. c. Измените параметры в расписании и нажмите на Сохранить.
Создание расписания	В представлении Расписания щелкните по +Расписание и выполните шаги по созданию расписания.

3. Необязательно: Чтобы сконфигурировать параметры расписания, которые не видны в компоненте Центр операций, используйте серверную команду. Например, вы можете счесть целесообразным запланировать операцию клиента, которая создает резервную копию определенного каталога и назначает для него класс управления, отличающийся от класса управления по умолчанию.
   a. На странице Обзор в компоненте Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
   b. Введите команду DEFINE SCHEDULE, чтобы создать расписание, или команду UPDATE SCHEDULE, чтобы изменить расписание. Дополнительные сведения о командах смотрите в разделах DEFINE SCHEDULE (определение расписания выполнения административных команд) или UPDATE SCHEDULE (Изменить запланированное задание клиента).

Задачи, связанные с данной:
Настройка расписания для ежедневных операций

Регистрация клиентов

Зарегистрируйте клиент, чтобы убедиться, что он может соединиться с сервером, а сервер может защитить данные клиента.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию technote 7048963.
Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе Аутентификация пользователей с использованием базы данных Active Directory.

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды REGISTER NODE и задайте параметр USERID:

  ```
  register node имя_узла пароль userid=имя_узла
  ```

  где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе Регистрация узла.
- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центр операций. Сделайте следующее:
  a. В панели меню Центра операций выберите Клиенты.
  b. В таблице Клиенты щелкните по + Клиент.
  c. Выполните шаги в мастере Добавить клиент:
     i. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель Включить в области Дедупликация данных на стороне клиента.
     ii. В окне Конфигурация скопируйте значения TCPSERVERADDRESS, TCPPORT, NODENAME, и DEDUPLICATION.
     Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
     iii. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     iv. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     v. Щелкните по Добавить клиент.

Ссылки, связанные с данной:
Опция Tcpserveraddress
Опция Tcpport
Опция Nodename
Опция дедупликации

Установка и настройка клиентов

Чтобы начать защищать клиентский узел, нужно установить и сконфигурировать выбранную программу.

Процедура

Если вы уже установили программу, начните с шага 2.

1. Выполните одно из следующих действий.
   - Чтобы установить программу в приложении или на клиентском узле, выполните инструкции.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows Совет: Можно также обновить существующие клиенты при помощи Центр операций. Инструкции смотрите в разделе Планирование обновлений клиента.
IBM Spectrum Protect for Databases	▪ Установка Data Protection for Oracle ▪ Установка Data Protection for SQL Server в ядре сервера Windows
IBM Spectrum Protect for Mail	▪ Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) ▪ Установка Data Protection for IBM Domino в системе Windows (V7.1.0) ▪ Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Программа	Ссылка на инструкции
IBM Spectrum Protect Snapshot	▪ Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux ▪ Установка и обновление IBM Spectrum Protect Snapshot для VMware ▪ Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Enterprise Resource Planning	▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 ▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- Чтобы установить программу на клиентском узле виртуальной машины, выполните инструкции для выбранного типа резервного копирования.

Тип резервного копирования	Ссылка на инструкции
Если вы собираетесь создавать полные резервные копии VMware виртуальных машин, установите и сконфигурируйте клиент резервного копирования и архивирования IBM Spectrum Protect.	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows
Если вы собираетесь установить постоянные полные резервные копии виртуальных машин, установите и сконфигурируйте IBM Spectrum Protect for Virtual Environments и клиент резервного копирования и архивирования на одном и том же клиентском узле или на разных клиентских узлах.	▪ Электронная документация по продукту IBM Spectrum Protect for Virtual Environments Совет: Программу для IBM Spectrum Protect for Virtual Environments и для клиента резервного копирования и архивирования можно получить в пакете установки IBM Spectrum Protect for Virtual Environments.

2. Чтобы разрешить клиенту соединяться с сервером, добавьте или обновите значения опций TCPSERVERADDRESS, TCPPORT и NODENAME в файле опций клиента. Используйте значения, записанные вами при регистрации клиента (раздел Регистрация клиентов).
   - Если клиенты установлены в операционной системе AIX, Linux или Mac OS X, добавьте значения в файл системных опций клиента, dsm.sys.
   - Если клиенты установлены в операционной системе Windows, добавьте значения в файл dsm.opt.

   По умолчанию, файлы опций находятся в каталоге установки.
3. Если вы установили клиент резервного копирования и архивирования в операционной системе Linux или Windows, то установите служба управления клиентами на клиенте. Следуйте инструкциям в разделе Установка службы управления клиентом.
4. Сконфигурируйте клиент для выполнения запланированных операций. Следуйте инструкциям в разделе Конфигурирование клиента для выполнения запланированных операций.
5. Необязательно: Сконфигурируйте связь через брандмауэр. Следуйте инструкциям в разделе Конфигурирование взаимодействий между клиентом и сервером через брандмауэр.
6. Запустите тестовое резервное копирование, чтобы проверить, защищены ли данные, как вы планировали. Например, для клиента резервного копирования и архивирования выполните следующие шаги:
   a. Выберите на странице Клиенты компонента Центр операций клиент, для которого вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
   b. Убедитесь, что резервное копирование выполнено успешно и что нет ни предупреждений, ни сообщений об ошибках.
7. Следите за результатами запланированных операций клиента в компоненте Центр операций.

Дальнейшие действия

Если требуется изменить набор объектов для резервного копирования, выполните инструкции в разделе Изменение объема резервного копирования клиента.

Конфигурирование клиента для выполнения запланированных операций

Вы должны сконфигурировать и запустить планировщик клиента на клиентском узле. Планировщик клиента обеспечивает взаимодействие между клиентом и сервером, чтобы могли выполняться запланированные операции. Например, запланированные операции обычно включают в себя резервное копирование файлов с клиента.

Об этой задаче

Предпочтительный метод заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций. Приемник клиента управляет планировщиком клиента, чтобы планировщик запускался, только когда это требуется:

- Когда наступило время запросить сервер о следующей запланированной операции
- Когда наступило время запустить следующую запланированную операцию

Используя приемник клиента, вы можете сократить число фоновых процессов на клиенте и помочь избежать проблем сохранения памяти.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, следуйте инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Если на вашем предприятии используется сторонний инструмент планирования в качестве стандартной практики, можно использовать этот инструмент планирования как альтернативу приемнику клиентов. Как правило, сторонние инструменты планирования запускают программы-клиенты напрямую, используя команды операционной системы. Чтобы сконфигурировать сторонний инструмент планирования, смотрите документацию по продукту.

Процедура

Чтобы сконфигурировать и запустить планировщик клиента с использованием приемника клиента, следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.
c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

   ```
   dsmc query sess
   ```

f. Запустите приемник клиента, введя в командной строке следующую команду:

   ```
   /usr/bin/dsmcad
   ```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте в файл запуска системы (обычно, /etc/inittab) следующую запись:

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Демон Client Acceptor
   ```

Linux

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.

c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

f. Запустите приемник клиента, войдя в систему от имени ID пользователя root и введя следующую команду:

```
service dsmcad start
```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте службу, введя в командной строке оболочки следующую команду:

```
# chkconfig --add dsmcad
```

MAC OS X

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Чтобы планировщик мог запускаться без участия оператора, щелкните по Авторизация, выберите Генерирование пароляи щелкните по Применить.
c. Чтобы указать, как осуществляется управление службами, щелкните по Веб-клиент, выберите Расписание, щелкните по Применить и выберите OK.
d. Чтобы сгенерированный пароль был сохранен, перезапустите клиент резервного копирования и архивирования.
e. Используйте для запуска приемника клиента приложение Инструменты IBM Spectrum Protect для администраторов.

Windows

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Утилиты > Мастер настройки > Помочь мне сконфигурировать Планировщик клиента. Щелкните по Далее.
b. Прочтите информации на странице мастера планировщика и нажмите Далее.
c. На странице Задача планировщика выберите Установить новый или дополнительный планировщик и нажмите Далее.
d. На странице Имя и расположение планировщика задайте имя для добавляемого планировщика клиента. Затем выберите Использовать Client Acceptor Daemon (CAD), чтобы управлять планировщиком, и нажмите Далее.
e. Введите имя, которое вы хотите присвоить этому приемнику клиента. Имя по умолчанию - Client Acceptor. Щелкните по Далее.
f. Выполните конфигурирование, выполняя шаги в мастере.
g. Обновите файл опций клиента, dsm.opt, и задайте для опции passwordaccess значение generate.
h. Чтобы сохранить пароль клиентского узла, введите в командной строке следующую команду:

```
dsmc query sess
```

Когда вам это предложат, введите пароль клиентского узла.
i. Запустите службу приемника клиента из панели Управление службами. Например, если вы использовали имя по умолчанию, запустите Служба Client Acceptor. Не запускайте службу планировщика, заданную вами на странице Имя и местонахождение планировщика. Служба планировщика автоматически запускается и останавливается службой приемника клиента по мере необходимости.

Конфигурирование взаимодействий между клиентом и сервером через брандмауэр

Если клиент должен связываться с сервером через брандмауэр, нужно включить связь между клиентом и сервером через брандмауэр.

Прежде чем начать

Если для регистрации клиентов вы использовали мастер добавления клиентов, найдите в файле опций клиента значения опций, полученные вами в ходе этого процесса. Для указания портов можно использовать значения.

Об этой задаче

Внимание: Не конфигурируйте брандмауэр, используя метод, который мог бы вызвать прекращение сеансов, используемых сервером или агентом хранения. Прекращение действительного сеанса может вызвать непредсказуемые последствия. Может показаться, что процессы и сеансы остановились из-за ошибок ввода-вывода. Чтобы помочь исключить сеансы из ограничений тайм-аута, сконфигурируйте известные порты для компонентов IBM Spectrum Protect. Убедитесь что для серверной опции KEEPALIVE осталось заданным значение по умолчанию YES. Это поможет вам убедиться, что связи клиент/сервер не прерывается. Инструкции относительно того, как задать опцию сервера KEEPALIVE смотрите в разделе KEEPALIVE.

Процедура

Откройте следующие порты, чтобы разрешить доступ через брандмауэр:

Порт TCP/IP для клиента резервного копирования и архивирования, административного клиента командной строки и планировщика клиента
: Задайте порт, используя опцию tcpport в файле опций клиента. Опция tcpport в файле опций клиента должна совпадать с опцией TCPPORT в файле опций сервера. Значение по умолчанию - 1500. Если вы решите использовать какое-либо значение, отличающееся от значения по умолчанию, задайте число в диапазоне 1024-32767.

Порт HTTP для включения взаимодействий между веб-клиентом и удаленными рабочими станциями
: Задайте порт для удаленной рабочей станции, задав опцию httpport в файле опций клиента удаленной рабочей станции. Значение по умолчанию - 1581.

Порты TCP/IP для удаленной рабочей станции
: Значение по умолчанию равно 0 (ноль); оно указывает, что два свободных номера портов случайным образом назначаются удаленной рабочей станции. Если вы не хотите, чтобы номера портов назначались произвольным образом, задайте значения, задав опцию webports в файле опций клиента удаленной рабочей станции.

Порт TCP/IP для сеансов администрирования
: Задайте порт, на котором сервер ожидает требований установления сеансов административного клиента. Значение опции клиента tcpadminport должно совпадать с опцией сервера TCPADMINPORT. Таким способом вы сможете защитить административные сеансы в частной сети.

Управление операциями клиентов

Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.

Об этой задаче

В некоторых случаях ошибки клиентов можно устранить, остановив и перезапустив приемник клиента. Если клиентские узлы или ID администратора окажутся заблокированы, вы сможете устранить проблему, разблокировав клиентский узел или ID администратора, а затем переустановив пароль.

Подробные инструкции по выявлению и устранению ошибок клиентов смотрите в разделе Устранение проблем клиентов.

- Оценка ошибок в журналах ошибок клиентов
  Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.
- Остановка и перезапуск приемника клиента
  Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.
- Изменение паролей
  Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

- Изменение объема резервного копирования клиента
  При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Оценка ошибок в журналах ошибок клиентов

Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.

Прежде чем начать

Чтобы устранить ошибки на клиенте резервного копирования и архивирования в операционной системе Linux или Windows, убедитесь, что у вас установлена и запущена служба служба управления клиентами. Инструкции по установке смотрите в разделе Установка службы управления клиентом. Инструкции по проверке установки смотрите в разделе Проверка того, правильно ли установлена служба управления клиентами.

Процедура

Чтобы диагностировать и устранить ошибки клиента, выполните одно из следующих действий:

- Если служба служба управления клиентами установлена на клиентском узле, выполните следующие шаги:
  1. На странице обзора в компоненте Центр операций щелкните по Клиенты и выберите клиент.
  2. Щелкните по Сведения.
  3. На странице Сводка клиента щелкните по вкладке Диагностика.
  4. Прочтите полученные сообщения журнала.
     Советы:
     - Чтобы показать или скрыть панель Журналы клиента, дважды щелкните по строке Журналы клиента.
     - Чтобы изменить размер панели Журналы клиента, щелкните по строке Журналы клиента и перетащите ее в нужное положение.

     Если на странице Диагностика показаны рекомендации, выберите рекомендацию. В панели Журналы клиента сообщения журнала клиента, с которыми связаны рекомендации, выделены.

  5. Используйте рекомендации, чтобы устранить проблемы, указанные в сообщениях об ошибках.
     Совет: Рекомендации предоставляются не для всех сообщений клиентов.
- Если служба служба управления клиентами не установлена на клиентском узле, смотрите журналы ошибок установленного клиента.

Остановка и перезапуск приемника клиента

Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

Об этой задаче

В некоторых случаях ошибки планирования клиентов можно устранить, остановив и перезапустив приемник клиента. Чтобы запланированные операции могли выполняться на клиенте, приемник клиента должен работать. Например, если вы измените IP-адрес или имя домене сервера, вы должны будете перезапустить приемник клиента.

Процедура

Следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- Чтобы остановить приемник клиента, выполните следующие действия:
  a. Определите ID процесса приемника клиента, введя в командной строке следующую команду:

     ```
     ps -ef | grep dsmcad
     ```

Ознакомьтесь с выводом. В приведенном ниже примере выходной информации 6764 - это ID процесса приемника клиента:

```
root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
```

b. Введите следующую команду в командной строке:

```
kill -9 PID
```

где *PID* задает ID процесса приемника клиента.

- Чтобы запустить приемник клиента, введите в командной строке следующую команду:

```
/usr/bin/dsmcad
```

Linux

- Чтобы остановить приемник клиента (но не перезапускать его), введите следующую команду:

```
# service dsmcad stop
```

- Чтобы остановить и перезапустить приемник клиента, введите следующие команды:

```
# service dsmcad restart
```

MAC OS X

Выберите Приложения > Утилиты > Терминал.

- Чтобы остановить приемник клиента, введите следующую команду:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Чтобы запустить приемник клиента, введите следующую команду:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Чтобы остановить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Остановить и OK.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Запуск и OK.

Ссылки, связанные с данной:
Устранение проблем расписаний клиентов

Изменение паролей

Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

Процедура

Чтобы устранить ошибки паролей, выполните одно из следующих действий:

- Если клиент резервного копирования и архивирования установлен на клиентском узле, а пароль был потерян или забыт, выполните следующие шаги:
  1. Сгенерируйте новый пароль, введя команду UPDATE NODE:

```
update node имя_узла
новый_пароль forcepwreset=yes
```

где *имя_узла* - это клиентский узел, а *новый_пароль* - это пароль, который вы назначаете.

2. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
   Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

- Если администратор окажется заблокирован из-за проблем, связанных с паролем, выполните следующие шаги:
  1. Чтобы обеспечить администратору доступ к серверу, введите команду UNLOCK ADMIN. Инструкции смотрите в разделе UNLOCK ADMIN (разблокирование администратора).
  2. Задайте новый пароль, используя команду UPDATE ADMIN:

     ```
     update admin имя_администратора
     новый_пароль
     forcepwreset=yes
     ```

     где *имя_администратора* - это имя администратора, а *новый_пароль* - это пароль, который вы назначаете.
- Если клиентский узел заблокирован, выполните следующие шаги:
  1. Определите, почему клиентский узел заблокирован и нужно ли его разблокировать. Например, если клиентский узел окажется списан, он удаляется из производственной среды. Обратить операцию списания нельзя, и клиентский узел останется заблокированным. Клиентский узел также может оказаться заблокированным, если данные клиента являются предметом юридического изучения.
  2. Если вам нужно разблокировать клиентский узел, используйте команду UNLOCK NODE. Инструкции смотрите в разделе UNLOCK NODE (Разблокировать клиентский узел).
  3. Сгенерируйте новый пароль, введя команду UPDATE NODE:

     ```
     update node имя_узла
     новый_пароль forcepwreset=yes
     ```

     где *имя_узла* задает имя узла, а *новый_пароль* - это пароль, который вы назначаете.
  4. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
     Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

Изменение объема резервного копирования клиента

При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Об этой задаче

Исключение ненужных объектов из операций резервного копирования позволяет лучше контролировать объем пространства хранения, необходимого для операций резервного копирования, а также расходы на хранение. В зависимости от вашего пакета лицензирования вам, возможно, также удастся ограничить расходы, связанные с лицензированием.

Процедура

То, как вы изменяете масштаб операций по резервному копированию, зависит от продукта, установленного на клиентском узле:

- Для клиента резервного копирования и архивирования можно создать список включения-исключения, чтобы включить файлы, группы файлов или каталоги в операции резервного копирования или исключить их из этих операций. Чтобы создать список включения-исключения, следуйте инструкциям в разделе Создание списка include-exclude.

  Чтобы обеспечить непротиворечивое использование списка включения-исключения для всех клиентов одного типа, можно создать на сервере набор опций клиента, содержащий необходимые опции. Затем вы назначаете набор опций клиента каждому из клиентов того же типа. Дополнительные сведения смотрите в разделе Управление операциями клиента через наборы опций клиентов.

- Для клиента резервного копирования и архивирования можно задать объекты в операции инкрементного резервного копирования, используя опцию domain. Следуйте инструкциям в разделе Domain, опция.
- В случае других продуктов, чтобы указать, какие объекты включаются в операции резервного копирования, а какие - исключаются из этих операций, следуйте инструкциям в документации по продукту.

Управление обновлениями клиентов

Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Прежде чем начать

1. Прочтите требования к совместимости клиентов/серверов в разделе Техническое замечание 1053218. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены.
2. Узнайте о требованиях к системе для клиента в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
3. Если решение содержит агенты хранения или библиотечные клиенты, ознакомьтесь с информацией о совместимости агентов хранения и библиотечных клиентов с серверами, сконфигурированными в качестве менеджеров библиотек. Смотрите раздел Техническое замечание 1302789.

   Если вы собираетесь обновить менеджера библиотек и библиотечный клиент, сначала нужно обновить менеджера библиотек.

Процедура

Для обновления программного обеспечения выполните инструкции, перечисленные в следующей таблице.

Программа	**Ссылка на инструкции**
Клиент резервного копирования и архивирования IBM Spectrum Protect	• Планирование обновлений клиента
IBM Spectrum Protect Snapshot	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Databases	• Обновление Data Protection for SQL Server • Установка Data Protection for Oracle • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0) • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Установка и обновление Data Protection for VMware • Установка Data Protection for Microsoft Hyper-V

Списание клиентского узла

Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).

Об этой задаче

При запуске процесса списания сервер блокирует клиентский узел, чтобы помешать ему получить доступ к серверу. Файлы, принадлежащие клиентскому узлу, постепенно удаляются, и затем удаляется клиентский узел. Можно списать следующие типы клиентских узлов:

Клиентские узлы приложения
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Клиентские узлы компьютеров
: В число клиентских узлов компьютеров входят рабочие станции, серверы файлов NAS и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Простейший метод списания клиентского узла заключается в том, чтобы использовать Центр операций. Процесс списания выполняется в фоновом режиме. Если клиент сконфигурирован для репликации данных клиента, Центр операций, прежде чем списать клиент, автоматически удалит клиент из репликации на исходном и целевом серверах репликации. Совет: Либо можно списать клиентский узел, введя команду DECOMMISSION NODE или DECOMMISSION VM. Вы можете счесть целесообразным использовать этот метод в следующих случаях:

- Чтобы запланировать процесс списания на будущее или выполнить ряд команд, используя сценарий, задайте выполнение процесса списания в фоновом режиме.
- Чтобы производить мониторинг процесса списания с целью отладки, задайте выполнение процесса списания в фоновом режиме. Если вы запустите процесс в активном режиме, вам придется дождаться завершения процесса, прежде чем вы сможете перейти к другим задачам.

Процедура

Выполните одно из следующих действий.

- Чтобы списать клиент в фоновом режиме, используя Центр операций, выполните следующие действия:
  1. На странице Обзор для компонента Центр операций щелкните по Клиенты и выберите клиент.
  2. Выберите Еще > Списать.
- Чтобы списать клиентский узел, используя команду администрирования, выполните одно из следующих действий:
  - Чтобы списать клиентские узлы приложений или системные клиентские узлы в фоновом режиме, введите команду DECOMMISSION NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

    ```
    decommission node austin
    ```

  - Чтобы списать клиентские узлы приложений или системные клиентские узлы в активном режиме, введите команду DECOMMISSION NODE и задайте параметр `wait=yes`. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

    ```
    decommission node austin wait=yes
    ```

  - Чтобы списать виртуальную машину в фоновом режиме, введите команду DECOMMISSION VM. Например, если имя виртуальной машины - AUSTIN, файловое пространство - 7, а имя файлового пространства задано с помощью ID файлового пространства, введите следующую команду:

```
decommission vm austin 7 nametype=fsid
```

Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Чтобы списать виртуальную машину в активном режиме, введите команду DECOMMISSION VM и задайте параметр `wait=yes`. Например, введите следующую команду:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Дальнейшие действия

Следите за сообщениями об ошибках, которые могут появиться в пользовательском интерфейсе или в выходной информации команды сразу после запуска процесса.

Можно проверить, списан ли клиентский узел:

1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты.
2. В таблице Клиенты проверьте состояние в столбце Под угрозой:
   - Состояние DECOMMISSIONED (Списан) указывает, что узел списан.
   - Нулевое значение указывает, что узел не списан.
   - Состояние PENDING (Отложено) указывает, что узел списывается или процесс списания завершился неудачно.

   Совет: Если вы хотите определить состояние отложенного процесса списания, введите следующую команду:

   ```
   query process
   ```

3. Ознакомьтесь с выводом команды:
   - Если указано состояние для процесса списания, процесс выполняется. Например:

     ```
     query process

      Номер       Описание процесса                  Состояние процесса
       Число
     --------     --------------------     -------------------------------------------
            3           DECOMMISSION NODE         Number of backup objects deactivated
                                                  for node NODE1: 8 objects deactivated.
     ```

   - Если для процесса списания никакого состояния не указано и вы не получили сообщения об ошибке, процесс не завершен. Процесс может быть не завершен, если файлы, связанные с узлом, еще не деактивированы. После деактивации файлов снова запустите процесс списания.
   - Если для процесса списания никакого состояния не указано и вы получили сообщения об ошибке, это означает, что процесс завершился неудачно. Еще раз запустите процесс списания.

Ссылки, связанные с данной:
DECOMMISSION NODE (Списать клиентский узел)
DECOMMISSION VM (Списать виртуальную машину)

Деактивация данных для высвобождения пространства хранения

В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Об этой задаче

Некоторые клиенты приложений всегда сохраняют данные на сервере как активные резервные копии данных. Поскольку активные резервные копии данных не управляются политиками устаревания перечня, данные не удаляются

автоматически, и серверное хранилище используется до бесконечности. Чтобы высвободить пространство хранения, используемое устаревшими данными, можно деактивировать данные.

Когда вы запускаете процесс деактивации, все активные резервные копии данных, сохраненные до указанной даты, станут неактивными. Данные будут удалены по мере истечения срока их хранения, и восстановить их будет нельзя. Функция деактивации применяется только к клиентам приложений, которые защищают базы данных Oracle.

Процедура

1. На странице обзора в компоненте Центр операций щелкните по Клиенты.
2. В таблице Клиенты выберите один или несколько клиентов и щелкните по Еще > Очистить.
   Метод командной строки: Деактивируйте данные, используя команду DEACTIVATE DATA.

Ссылки, связанные с данной:
DEACTIVATE DATA (деактивация данных для клиентского узла)

Управление хранилищем данных

Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.

- Аудит контейнера пула хранения
  Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе данных и в контейнере в пуле хранения.
- Управление емкостью перечня
  Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.
- Управление использованием памяти и процессора
  Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.
- Тонкая настройка запланированных операций
  Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Ссылки, связанные с данной:
Типы пулов хранения

Аудит контейнера пула хранения

Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе данных и в контейнере в пуле хранения.

Об этой задаче

Вы производите аудит пулов хранения контейнеров в следующих случаях:

- При вводе команды QUERY DAMAGED обнаруживается ошибка
- Сервер выводит на экран сообщения о поврежденных экстентах данных
- Ваше оборудование сообщает о проблеме, и появляются сообщения об ошибках, связанные с пулом хранения контейнера

Процедура

1. Чтобы произвести аудит пула хранения на основе контейнеров, введите команду AUDIT CONTAINER. Например, введите следующую команду, чтобы произвести аудит контейнера, 000000000000076c.dcf:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Прочтите выходные данные сообщения ANR4891I, чтобы получить информацию о всех поврежденных экстентах данных.

Дальнейшие действия

При обнаружении проблем с пулом хранения контейнера вы можете восстановить данные на основе вашей конфигурации. Введите команду AUDIT CONTAINER и задайте имя контейнера.

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения каталогов-контейнеров или в облачно-контейнерном пуле хранения)

Управление емкостью перечня

Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

Прежде чем начать

У активного и архивного журналов есть следующие особенности:

- Максимальный размер активного журнала равен 512 ГБ. Более подробную информацию о размерах активного журнала для вашей системы смотрите в разделе Планирование массивов хранения.
- Размер архивного журнала ограничен размером файловой системы, в которой он установлен. Размер архивного журнала не поддерживается на заранее заданном уровне, как в случае активного журнала. Архивные файлы журналов автоматически удаляются, когда они становятся больше не нужны.

(Необязательно) Лучше всего создать архивный журнал отказоустойчивости, чтобы сохранять файлы архивного журнала при переполнении каталога архивных журналов.

Проверьте Центр операций, чтобы определить, какой компонент перечня переполняется. Прежде чем увеличивать размер одного из компонентов перечня, убедитесь, чтобы вы остановили сервер.

Процедура

- Чтобы увеличить размер базы данных, выполните следующие шаги:
  - Создайте один или несколько каталогов для базы данных на отдельных накопителях или в файловых системах.
  - Введите команду EXTEND DBSPACE, чтобы добавить каталог или каталоги к базе данных. Каталоги должны быть доступны для ID пользователя экземпляра менеджера базы данных. По умолчанию данные перераспределяются по всем каталогам базы данных и пространство высвобождается.
    Советы:
    - Время, необходимое для полного перераспределения данных и высвобождения пространства, изменяется в зависимости от размера вашей базы данных. Убедитесь, что это учтено при планировании.
    - Убедитесь, что размер указанных каталогов совпадает с размером существующих каталогов, чтобы обеспечить согласованную степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.
  - Остановите и перезапустите сервер для полного использования новых каталогов.
  - Если потребуется, исправьте базу данных. Реорганизация индекса и таблиц для базы данных сервера может помочь избежать неожиданных проблем, связанных с ростом базы данных и производительностью. Дополнительную информацию о реорганизации базы данных смотрите в Техническое замечание 1683633.
- Чтобы уменьшить размер базы данных для серверов V7.1 и новее, введите следующие команды DB2 из каталога экземпляра сервера:
  Ограничение: Команды могут увеличить число операций ввода-вывода и повлиять на производительность сервера. Чтобы свести к минимуму проблемы производительности, подождите выполнения одной команды перед вводом следующей команды. Команды DB2 можно вводить, когда сервер работает.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
```

```
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Чтобы увеличить или уменьшить размер активного журнала, выполните следующие шаги:
  1. Убедитесь, что в каталоге активного журнала достаточно пространства для увеличения размера журнала. Если существует зеркальная копия журнала, там, где она находится, также должно быть достаточно места для увеличения размера журнала.
  2. Отключите сервер.
  3. Измените в файле dsmserv.opt значение опции ACTIVELOGSIZE, задав новый размер активного журнала (в мегабайтах).
     Размер файла активного журнала основан на значении опции ACTIVELOGSIZE. Рекомендации по требованиям к объему пространства приведены в следующей таблице:

     Табл. 1. Как оценить требования к пространству томов и файлов

Значение опции ACTIVELOGSize	**Зарезервируйте этот объем свободного пространства в каталоге активного журнала в дополнение к пространству ACTIVELOGSize.**
16 ГБ - 128 ГБ	5120 МБ
129 ГБ - 256 ГБ	10240 МБ
257 ГБ - 512 ГБ	20480 МБ

     Чтобы изменить размер активного журнала до максимального размера, равного 512 ГБ, введите следующую серверную опцию:

     ```
     activelogsize 524288
     ```

  4. Если вы собираетесь использовать новый каталог активного журнала, измените имя каталога, заданное серверной опцией ACTIVELOGDIRECTORY. Новый каталог должен быть пустым, и он должен быть доступен для ID пользователя менеджера базы данных.
  5. Перезапустите сервер.
- Произведите сжатие архивных журналов, чтобы уменьшить объем пространства, необходимого для хранения. Разрешите динамическое сжатие архивного журнала следующей командой:

  ```
  setopt archlogcompress yes
  ```

  Ограничение: Будьте внимательны, если вы разрешаете опцию сервера ARCHLOGCOMPRESS на компьютерах с постоянным высоким использованием томов и высокими рабочими нагрузками. Разрешение этой опции в такой среде может привести к задержкам при архивировании файлов журнала из файловой системы активного журнала в файловую систему архивного журнала. Задержка может привести к тому, что в файловой системе активного журнала не хватит места. Обязательно выполняйте мониторинг пространства, доступного в файловой системе активного журнала, после разрешения сжатия архивного журнала. Если использование файловой системы каталога активного журнала приближается к предельному, то запретите опцию сервера ARCHLOGCOMPRESS. Чтобы немедленно запретить сжатие архивного журнала без остановки сервера, введите команду SETOPT.

Ссылки, связанные с данной:
ACTIVELOGSIZE, серверная опция
EXTEND DBSPACE (увеличение емкости базы данных)
SETOPT (Задать динамическое обновление серверной опции)

Управление использованием памяти и процессора

Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.

Прежде чем начать

- Убедитесь, что в вашей конфигурации используются необходимые аппаратные и программные средства. Дополнительные сведения смотрите в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
- Дополнительную информацию об управлении ресурсами (например, база данных и журнал восстановления) смотрите в разделе Планирование массивов хранения.
- Добавьте больше системной памяти, чтобы определить, повышается ли при этом производительность. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память.

Процедура

1. Высвобождайте память из кэша файловой системы, если это возможно.
2. Для управления системной памятью, используемой каждым сервером в системе, используйте опцию DBMEMPERCENT. Ограничьте процентную долю системной памяти, которая может использоваться менеджером базы данных каждого сервера. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.
3. Задайте для базы данных предельный объем данных пользователя и собственной памяти, чтобы не вырабатывать собственную память. Если собственная память будет исчерпана, это может приводить к ошибкам, снижению производительности ниже оптимальной и нестабильности.

Тонкая настройка запланированных операций

Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Процедура

1. Регулярно отслеживайте производительность системы, чтобы убедиться, что задачи по резервному копированию и обслуживанию выполняются успешно. Дополнительную информацию о мониторинге смотрите в разделе Мониторинг решения с одной площадкой.
2. Если информация мониторинга показывает, что рабочая нагрузка сервера повышается, вам, возможно, следует проверить информацию планирования. Проверьте, является ли емкость системы достаточной, в следующих случаях:
    - Число клиентов увеличивается
    - Объем данных, резервное копирование которых производится, возрастает
    - Время, доступное для резервного копирования, изменяется
3. Определите, есть ли в вашем решении проблемы, отрицательно влияющие на производительность. Проверьте расписания клиентов, чтобы выяснить, выполняются ли задачи в течение запланированного периода времени:
    a. Выберите клиента на странице Клиенты Центра операций.
    b. Щелкните по Сведения.
    c. На странице Сводка на клиенте проверьте операции Создана резервная копия и Реплицирован, чтобы выявить все риски.

    Скорректируйте время и частоту операций резервного копирования клиента, если потребуется.
4. Запланируйте достаточно времени для следующих задач по обслуживанию, чтобы они успешно выполнялись в течение 24-часового периода:
    a. Создание резервной копии базы данных
    b. Запускайте обработку устаревания, чтобы удалить резервные и архивные копии файлов из серверного хранилища.

Понятия, связанные с данным:
Производительность
Задачи, связанные с данной:

Дедупликация данных (V7.1.1)

Защита сервера IBM Spectrum Protect

Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.

- Понятия, касающиеся защиты
  Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.
- Управление администраторами
  Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.
- Изменение требований к паролям
  Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.
- Защита сервера в системе
  Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Понятия, касающиеся защиты

Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.

Transport Layer Security

Можно использовать протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS), чтобы обеспечить защиту транспортного слоя для безопасной связи между серверами, клиентами и агентами хранения. Если вы пересылаете данные между сервером, клиентом и агентом хранения, используйте SSL или TLS для шифрования данных.

Совет: Любая документация IBM Spectrum Protect, обозначенная как "SSL" или "выбрать SSL", применима к TLS.

SSL предоставляется Global Security Kit (GSKit), установленным с сервером IBM Spectrum Protect и используемым сервером, клиентом и агентом хранения.

Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных DB2, который используется какими-либо серверами IBM Spectrum Protect.

Каждый сервер, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатором (certificate authority, CA). Вы можете использовать свои собственные сертификаты или можете приобрести сертификаты у сертификатора (CA). Любой сертификат нужно установить и добавить к базе данных ключей для сервера IBM Spectrum Protect, клиента или агента хранения. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL. Некоторые сертификаты сертификаторов предварительно устанавливаются в базах данных ключей по умолчанию.

SSL устанавливается независимо от сервера IBM Spectrum Protect, клиента и агента хранения.

Уровни полномочий

При использовании каждого сервера IBM Spectrum Protect существует ряд доступных уровней административных полномочий, определяющих задачи, которые может выполнить администратор.

После регистрации администратору нужно предоставить полномочия, назначив для него один или несколько уровней административных полномочий. Администратор с системными полномочиями может выполнить любую задачу с сервером и назначить уровни полномочий для других администраторов, воспользовавшись командой GRANT AUTHORITY. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Администратор может зарегистрировать другие ID администраторов, предоставить им уровни полномочий, переименовать или удалить их, а также блокировать или разблокировать их доступ к серверу.

Администратор может управлять доступом к определенным клиентским узлам для ID пользователей root и ID пользователей, не являющихся пользователями root. По умолчанию, ID пользователя, не являющегося пользователем root, не может производить резервное копирование данных на узле. Используйте команду UPDATE NODE, чтобы изменить параметры узла и включить резервное копирование.

Пароли

По умолчанию сервер автоматически использует аутентификацию с помощью пароля. Если аутентификация пароля включена (on), все пользователи при получении доступа к серверу должны указывать пароль.

Используйте Lightweight Directory Access Protocol (LDAP), чтобы применить более строгие требования к паролям. Дополнительную информацию смотрите в разделе Управление паролями и процедурами входа (V7.1.1).

Табл. 1. Характеристики аутентификации паролей

Характеристика	**Дополнительная информация**
Значение регистра символов	Без учета регистра.
Срок действия пароля по умолчанию	90 дней. Отсчет начинается с момента первой регистрации на сервере ID администратора или клиентского узла. Если в течение этого периода пароль не изменится, пароль нужно будет изменить, когда пользователь в следующий раз получит доступ к серверу.
Число попыток ввода неправильного пароля	Для всех клиентских узлов можно установить максимальное количество последовательных попыток неправильного ввода пароля. После превышения данного значения сервер блокирует такой узел.
Длина пароля по умолчанию	8 символов Администратор может задать минимальную длину. Начиная с версии 8.1.4, минимальная длина паролей сервера по умолчанию изменилась с 0 до 8 символов.

Защита сеанса

Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами и назначается с использованием параметра SESSIONSECURITY.

Для параметра SESSIONSECURITY можно задать одно из следующих значений:

- Значение STRICT принудительно применяет наиболее высокий уровень защиты взаимодействий между серверами IBM Spectrum Protect, узлами и администраторами.
- Значение TRANSITIONAL указывает, что при обновлении программы IBM Spectrum Protect до V8.1.2 или новее используется существующий протокол связи. Это значение по умолчанию. Если задано SESSIONSECURITY=TRANSITIONAL, автоматически применяются более строгие параметры защиты при использовании более высоких версий протокола TLS и при обновлении программы до V8.1.2 или новее. После того как узел, администратор или сервер будет соответствовать требованиям для значения STRICT, защита сеанса автоматически обновится до значения STRICT, и объект больше не сможет проходить аутентификацию, исплользуя предыдущую версию клиента или более ранние протоколы TLS.
  Прим.: До обновления серверов обновлять клиенты резервного копирования и архивирования до V8.1.2 или новее не нужно. После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжат взаимодействовать с сервером, используя значение TRANSITIONAL, пока объект будет соответствовать требованиям для значения STRICT. Точно так же можно обновить клиенты резервного копирования и архивирования до V8.1.2 или новее до обновления серверов IBM Spectrum Protect, но обновлять серверы сначала не требуется. Связь между серверами и клиентами не прерывается.

Дополнительные сведения о значениях параметра SESSIONSECURITY смотрите в описаниях следующих команд.

Табл. 2. Команды, используемые, чтобы задать параметр SESSIONSECURITY

Объект	**Команда**

Объект	Команда
Клиентские узлы	• REGISTER NODE • UPDATE NODE
Администраторы	• REGISTER ADMIN • UPDATE ADMIN
Серверы	• DEFINE SERVER • UPDATE SERVER

Администраторы, прошедшие аутентификацию с использованием команды DSMADMC, команды DSMC или программы dsm, после аутентификации с использованием V8.1.2 или новее не смогут проходить аутентификацию с использованием более ранней версии. Чтобы устранить проблемы аутентификации администраторов, смотрите следующие советы:
Советы:

- Убедитесь, что все программы IBM Spectrum Protect, используемые учетной записью администратора для входа в систему, обновлены до V8.1.2 или новее. Если учетная запись администратора производит вход из нескольких систем, убедитесь, что сертификат сервера установлен в каждой системе.
- После того как администратор пройдет аутентификацию на сервере V8.1.2 или новее, используя клиент V8.1.2 или новее, администратор сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. Команду администратора можно вводить из любой системы.
- Если потребуется, создайте отдельную учетную запись администратора, чтобы использовать ее только при работе с клиентами и серверами, на которых работает V8.1.1 или более ранняя программа.

Принудительно примените наивысший уровень защиты взаимодействий с сервером IBM Spectrum Protect, сделав так, чтобы все узлы, администраторы и серверы использовали защиту сеанса STRICT. Можно воспользоваться командой SELECTЮ чтобы определить, какие серверы, узлы и администраторы используют защиту сеанса TRANSITIONAL, чтобы их обновить для использования защиты сеанса STRICT.

Задачи, связанные с данной:
Защита связи

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Процедура

Чтобы изменить параметры администратора, выполните описанные ниже шаги.

Задача	Процедура

Добавить администратора	Чтобы добавить администратора, ADMIN1, с системными полномочиями и задать пароль, выполните следующие шаги:
	a. Зарегистрируйте администратора и задайте Pa$#$twO в качестве пароля, введя следующую команду:
	`register admin admin1 Pa$#$twO`
	b. Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`

Задача	Процедура

Изменить административные полномочия	Измените уровень полномочий для администратора ADMIN1.
	• Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`
	• Аннулируйте системные полномочия администратора, введя следующую команду:
	`revoke authority admin1 classes=system`

Удалить администраторов	Аннулируйте для администратора ADMIN1 доступ к серверу IBM Spectrum Protect, введя следующую команду: `remove admin admin1`
Временно запретите доступ к серверу	Заблокируйте или разблокируйте администратора, введя команду LOCK ADMIN или UNLOCK ADMIN.

Изменение требований к паролям

Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.

Об этой задаче

Применяя аутентификацию на основе паролей и управляя ограничениями паролей, вы защищаете данные и серверы от потенциальных угроз безопасности.

Процедура

Чтобы изменить требования к паролям для серверов IBM Spectrum Protect, выполните описанные ниже задачи.

Табл. 1. Задачи по аутентификации для серверов IBM Spectrum Protect

Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число неудачных попыток в поле Предел неудачных попыток входа в систему. Значение по умолчанию при установке равно 0.
Задайте минимальную длину пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число символов в поле Минимальная длина пароля.
Задайте срок действия паролей.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте срок в днях в поле Общий срок действия паролей.

Задача	Процедура
Отключите аутентификацию на основе паролей.	По умолчанию сервер автоматически использует аутентификацию с помощью пароля. При аутентификации пароля все пользователи для получения доступа к серверу должны вводить пароль. Запретить аутентификацию пароля можно только для паролей, аутентификация которых выполняется на сервере (LOCAL). Отключая аутентификацию на основе паролей, вы делаете сервер доступным для угроз безопасности.

Задать метод аутентификации по умолчанию.	Введите команду SET DEFAULTAUTHENTICATION. Например, чтобы использовать сервер как метод аутентификации по умолчанию, введите следующую команду:
	
	`set defaultauthentication local`
	
	Чтобы обновить клиентский узел для аутентификации на сервере, включите `AUTHENTICATION=LOCAL` в команду UPDATE NODE:
	
	`update node authentication=local`

Понятия, связанные с данным:

Аутентификация пользователей IBM Spectrum Protect с использованием сервера LDAP

Управление паролями и процедурами входа (V7.1.1)

Защита сервера в системе

Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Процедура

Убедитесь, что неавторизованные пользователи не могут получить доступ к каталогам для базы данных сервера и экземпляра сервера. Оставьте для этих каталогов параметры доступа, которые вы сконфигурировали во время реализации.

- Ограничение доступа пользователей к серверу
  Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.
- Ограничение доступа путем ограничений портов
  Ограничьте доступ к серверу, применив ограничения портов.

Ограничение доступа пользователей к серверу

Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Процедура

1. После регистрации администратора с использованием команды REGISTER ADMIN используйте команду GRANT AUTHORITY, чтобы задать уровень полномочий администратора. Дополнительные сведения о том, как задавать и изменять полномочия, смотрите в разделе Управление администраторами.
2. Чтобы управлять полномочиями администратора на выполнение некоторых задач, используйте следующие две опции сервера:
   a. Вы можете задать уровень полномочий, который должен быть у администратора, чтобы он мог ввести команды QUERY и SELECT с опцией сервера QUERYAUTH. По умолчанию, не требуется никакого уровня полномочий. Данное требование можно изменить, указав один из уровней полномочий, включая системные.

b. Вы можете указать, что для команд, которые заставляют сервер записывать внешний файл за счет использования серверной опции REQSYSAUTHOUTFILE, требуются системные полномочия. По умолчанию, для выполнения таких команд необходимы системные полномочия.

3. Можно ограничить резервное копирование данных на клиентском узле, так чтобы его могли выполнять только ID пользователя root или авторизованные пользователи. Например, чтобы ограничить резервное копирование ID пользователя root, введите команду REGISTER NODE или UPDATE NODE и задайте параметр BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Ограничение доступа путем ограничений портов

Ограничьте доступ к серверу, применив ограничения портов.

Об этой задаче

В зависимости от ваших требований к защите вам может потребоваться ограничить доступ к отдельным серверам. Сервер IBM Spectrum Protect можно настроить на прием данных с четырех портов TCP/IP: двух - для обычных протоколов TCP/IP или протоколов Secure Sockets Layer (SSL)/Transport Layer Security (TLS), и двух, которые можно использовать только для протокола SSL/TLS.

Процедура

Чтобы указать нужные порты, можно задать опции сервера (смотрите раздел Табл. 1).

Табл. 1. Опции сервера и доступ к портам

Серверный параметр	Доступ к портам
TCPPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для отслеживания требований установления сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. Значение по умолчанию - 1500.
TCPADMINPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований установления сеансов, отличных от сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. По умолчанию используется значение, заданное опцией TCPPORT. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.
SSLTCPPORT	Задает адрес порта TCP/IP SSL для сервера. Этот порт принимает только сеансы с поддержкой SSL. Значения порта по умолчанию нет.
SSLTCPADMINPORT	Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает требования на установление сеансов SSL. Значения порта по умолчанию нет. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.

ограничения:
Следующие ограничения применяются при определении портов сервера только для SSL (SSLTCPPORT и SSLTCPADMINPORT):

- Если вы задаете порт сервера только SSL в параметре LLADDRESS в команде DEFINE SERVER или UPDATE SERVER, надо также задать параметр SSL=Yes.
- Если вы задаете порт сервера только SSL для опции TCPPORT клиента, то надо также задать YES для опции SSL клиента.

Ссылки, связанные с данной:
Планирование доступа через брандмауэр

Остановка и запуск сервера

Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите

сервер в производственном режиме.

Прежде чем начать

Чтобы остановить и запустить сервер IBM Spectrum Protect, требуются системные полномочия или полномочия оператора.

- Остановка сервера
  Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.
- Запуск сервера для задач обслуживания или реконфигурирования
  Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Остановка сервера

Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

Об этой задаче

При вводе команды HALT для остановки сервера происходят следующие действия:

- Все процессы и сеансы узлов клиентов будут отменены.
- Все текущие транзакции будут остановлены. (При перезапуске сервера будет произведен откат транзакций.)

Процедура

Чтобы подготовить систему и остановить сервер, выполните следующие шаги:

1. Запретите запуск новых сеансов клиентских узлов, введя команду DISABLE SESSIONS:

   ```
   disable sessions all
   ```

2. Определите, не выполняются ли какие-либо сеансы клиентских узлов или процессы, выполнив следующее:
   a. На странице Центра операций Обзор посмотрите в области Активность общее число процессов и сеансов, которые активны в настоящий момент. Если это число заметно отличается от значения, которое обычно показано во время повседневного управления хранением, то просмотрите другие индикаторы состояния в Центре операций, чтобы определить, ошибка ли это.
   b. Смотрите график в области Активность, чтобы сравнить объем сетевого трафика за следующие периоды:
      - Текущий период, то есть, самые последние 24 часа
      - Предыдущий период, то есть, за 24 часа до текущего периода

      Если на графике за предыдущий период показано ожидаемый объем трафика, существенные различия с графиком за текущий период могут указывать на проблему.
   c. Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения. Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, получите информацию о процессах при помощи команд администрирования. Введите команду QUERY PROCESS для запроса процессов и получения информации о сеансах при помощи команды QUERY SESSION.
3. Дождитесь завершения сеансов клиентских узлов или отмените их. Чтобы отменить процессы и сеансы, сделайте следующее:
   - Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   - Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   - Нажмите кнопку Отмена.
   - Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, отмените сеансы при помощи команд администрирования. Введите команду CANCEL SESSION, чтобы отменить сеанс и процессы при помощи команды CANCEL PROCESS.

Совет: Если процесс, который вы хотите отменить, ожидает монтирования ленточного тома, требование монтирования будет отменено. Например, если вы введете команду EXPORT, IMPORT или MOVE DATA, команда может инициировать процесс, для которого потребуется смонтировать ленточный том. Однако, если ленточный том монтируется автоматизированной библиотекой, операция отмены может не иметь силы, пока не завершится процесс монтирования. В зависимости от вашей системной среды на это может потребоваться несколько минут.

4. Остановите сервер с помощью команды HALT:

```
halt
```

Запуск сервера для задач обслуживания или реконфигурирования

Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

```
halt
```

2. Запустите сервер, используя метод, который вы используете в производственном режиме. Выполните инструкции для вашей операционной системы.
   - Операционные системы AIXЗапуск экземпляра сервера
   - Операционные системы LinuxЗапуск экземпляра сервера
   - Операционные системы WindowsЗапуск экземпляра сервера

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Планирование обновления сервера

Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.

Об этой задаче

Выполните следующие рекомендации:

- Предпочтительный метод - обновить сервер с использованием мастера установки. Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.
- Если доступны обновления и для серверного компонента, и для компонента Центр операций, выберите переключатели, указывающие, что нужно обновить оба компонента.

Процедура

1. Проверьте список пакетов исправлений и промежуточных исправлений. Смотрите раздел Техническое замечание 1239415.
2. Ознакомьтесь с усовершенствованиями продукта, описанными в файлах readme.
   Совет: Получив пакет установки со страницы сайт поддержки IBM Spectrum Protect, вы также сможете получить доступ к файлу readme.
3. Убедитесь что версия, до которой вы обновляете сервер, совместима с другими компонентами, например, с агентами хранения и клиентами библиотек. Смотрите раздел Техническое замечание 1302789.
4. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены. Смотрите раздел Техническое замечание 1053218.
5. Прочтите инструкции по обновлению. Обязательно создайте резервную копию базы данных сервера, информации о конфигурации устройств и файла хронологии томов.

Дальнейшие действия

Чтобы установить пакет исправлений или промежуточное исправление, следуйте инструкциям для вашей операционной системы:

- Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect

Информация, связанная с данной:
Процесс обновления и перенастройки - Часто задаваемые вопросы

Подготовка к отключению или обновлению системы

Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.

Об этой задаче

Убедитесь, что вы запланировали регулярные действия по управлению, защите и обслуживанию сервера.

Процедура

1. Отмените выполняющиеся процессы и сеансы, сделав следующее:
   a. Выберите в Центр операций на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   b. Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   c. Нажмите кнопку Отмена.
2. Остановите сервер с помощью команды HALT:

```
halt
```

Совет: Можно ввести команду halt из Центр операций, установив указатель мыши на значок Параметры и щелкнув по Построитель команд. Затем выберите сервер, введите `halt` и нажмите на клавишу ввода (Enter).

Реализация плана аварийного восстановления

Примените стратегию аварийного восстановления, чтобы восстановить приложения, если произойдет авария, и обеспечить высокую доступность сервера.

Об этой задаче

Определите требования к восстановлению после аварии, выявив бизнес-приоритеты для восстановления клиентского узла, системы, которые вы используете для восстановления данных, и то, есть ли у клиентских узлов соединение с сервером восстановления. Используйте репликацию и защиту пулов хранения для защиты ваших данных. Также нужно определить, как часто производится защита пулов хранения на основе каталогов-контейнеров.

- Выполнение отработки восстановления
  Запланируйте отработку аварийного восстановления, чтобы подготовиться к аудиту, удостоверяющему возможность восстановления сервера IBM Spectrum Protect и гарантирующему, что можно восстановить данные и возобновить операции после перебоя с питанием. Отработка также поможет вам убедиться, что можно восстановить все данные и возобновить операции, прежде чем возникнет критическая ситуация.

Восстановление после перебоев в работе системы

В случае дисковых решений IBM Spectrum Protect с одной площадкой можно только восстановить перечень на локальном компьютере и восстановить базу данных, чтобы защитить ваши данные.

Процедура

Используйте один из следующих методов, чтобы восстановить перечень на локальной площадке в зависимости от типа информации в резервной копии.
Ограничение: Поскольку у дисковых решений с одной площадкой нет второй копии пула хранения, вы не сможете восстановить пулы хранения. Чтобы проверить архитектуру дисковых решений, смотрите раздел Выбор решения IBM Spectrum Protect для вашей среды.

Табл. 1. Сценарии восстановления после аварии

Сценарий	**Процедура**
Ваша система недоступна, и вы хотите восстановить на локальном компьютере более раннюю версию, используя системные инструменты.	• Используйте IBM Spectrum Protect, чтобы создать резервную копию сервера на другом сервере. • Используйте инструменты операционной системы, чтобы произвести резервное копирование вашей системы и восстановить ее до более ранней версии.
Произошли отключение питания или авария, и вы хотите восстановить свои данные из резервных версий данных.	• Чтобы создать резервную копию клиента, на странице Клиенты TSM в компоненте Центр операций выберите клиенты, резервные копии которых вы хотите создать, и щелкните по Резервное копирование. • На странице Серверы TSM в компоненте Центр операций выберите сервер, для базы данных которого вы хотите создать резервную копию. Щелкните по Резервное копирование и выполните инструкции в окне Резервное копирование базы данных сервера. Чтобы восстановить пул хранения из резервной копии версии пула хранения, нужно восстановить базу данных. Введите команду DSMSERV RESTORE DB, чтобы восстановить базу данных и связанные пулы хранения в резервной копии версии.

- Восстановление базы данных
  Возможно, вам придется восстанавливать базу данных IBM Spectrum Protect после аварии. Вы можете восстановить базу данных до наиболее актуального состояния или на указанный момент времени. Для восстановления базы данных у вас должны быть тома с полной или инкрементной копией базы данных или с моментальным снимком резервной копии базы данных.

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
DSMSERV RESTORE DB (восстановление базы данных)

Решение с несколькими площадками

Это решение по защите данных обеспечивает репликацию на нескольких площадках, чтобы каждый сервер защищал данные для другой площадки.

- Планирование дискового решения по защите данных с несколькими площадками
  Спланируйте решение с несколькими площадками по защите данных на диске с участием серверов на двух площадках, где используется дедупликация и репликация данных.
- Реализация решения по защите данных на диске для нескольких площадок
  Дисковое решение с несколькими площадками конфигурируется на двух площадках и использует дедупликацию данных и репликацию.
- Мониторинг дискового решения с несколькими площадками
  После реализации дискового решения IBM Spectrum Protect с несколькими площадками произведите мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.
- Управление операциями для дискового решения с несколькими площадками
  Используйте эту информацию для управления операциями при дисковом решении для нескольких площадок с IBM Spectrum Protect, включающим в себя сервер и использующим дедупликацию данных для нескольких площадок.

Планирование дискового решения по защите данных с несколькими площадками

Спланируйте решение с несколькими площадками по защите данных на диске с участием серверов на двух площадках, где используется дедупликация и репликация данных.

Методы реализации

Серверы можно сконфигурировать для дискового решения с несколькими площадками следующими способами:

Конфигурирование серверов с использованием компонента Центр операций и административных команд
: Можно сконфигурировать диапазон систем хранения и программы сервера для вашего решения. Задачи по конфигурированию выполняются при помощи мастеров и опций в командах Центр операций и IBM Spectrum Protect. Информацию о том, как начать работу смотрите в разделе Дорожная карта планирования.

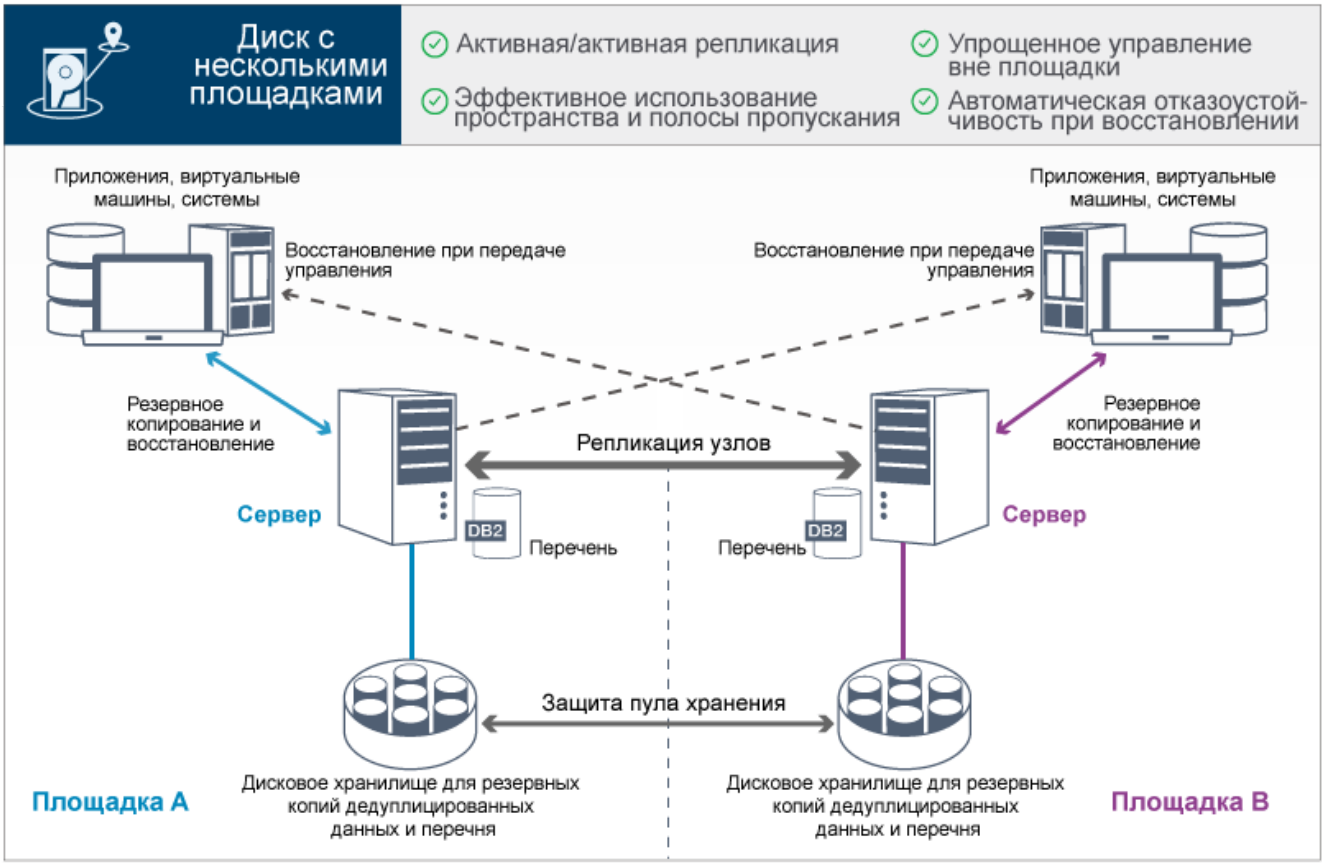
Сконфигурируйте серверы при помощи автоматизированных сценариев
: Подробные рекомендации по конфигурированию с использовангием конкретных систем хранения IBM® Storwize и автоматических сценариев по конфигурированию каждого сервера смотрите в IBM Spectrum Protect blueprints. Документация и сценарии доступны на сайте IBM developerWorks по адресу: IBM Spectrum Protect Blueprints.

  В проектной документации нет шагов по установке и конфигурированию Центр операций или по настройке защищенной связи с использованием Transport Security Layer (TLS). Репликация конфигурируется при помощи команд после настройки сервера. Включена возможность использования Elastic Storage Server на основе технологии IBM Spectrum Scale.

Дорожная карта планирования

Запланируйте дисковое решение с несколькими площадками, ознакомившись со схемой архитектуры, показанной ниже на рисунке, а затем выполнив задачи дорожной карты, которые приводятся после диаграммы.

Рис. 1. Решение с несколькими площадками



Описанные ниже шаги необходимы, чтобы правильно произвести планирование для дисковой среды с несколькими площадками.

1. Выберите размер системы.
2. Спланируйте площадки.
3. Выполните требования к аппаратному и программному обеспечению.
4. Запишите значения конфигурации системы в рабочие листы планирования.
5. Спланируйте хранение.
6. Спланируйте защиту.
    a. Спланируйте роли администраторов.
    b. Спланируйте защищенную связь.
    c. Спланируйте хранение шифрованных данных.
    d. Спланируйте доступ через брандмауэр.

Выбор размера системы

Выберите размер сервера IBM Spectrum Protect на основе объема данных, которыми вы управляете, и систем, которые нужно защитить.

Об этой задаче

Информацию в приведенной ниже таблице можно использовать, чтобы определить размер сервера, который вам потребуется, в зависимости от объема данных, которыми вы управляете.

В следующей таблице описан том данных, которым управляет сервер. Этот объем включает в себя все версии. Ежедневный объем данных - это объем данных, резервные копии которых вы создаете ежедневно. И общий объем управляемых данных, и ежедневный объем новых данных измеряются как размер до любого сокращения данных.

Табл. 1. Определение размера сервера

Общий объем управляемых данных	**Ежедневный объем новых данных для резервного копирования**	**Необходимый размер сервера**
60 ТБ - 240 ТБ	До 10 ТБ в день	Малое

Общий объем управляемых данных	Ежедневный объем новых данных для резервного копирования	Необходимый размер сервера
196 ТБ - 784 ТБ	10 - 20 ТБ в день	Среднее
1000 ТБ - 4000 ТБ	20 - 100 ТБ в день	Большое

Значения ежедневных резервных копий в таблице основаны на результатах испытаний с объектами по 128 МБ, которые используются компонентом IBM Spectrum Protect for Virtual Environments. Рабочие нагрузки, состоящие из объектов менее 128 КБ, могут не достигать этих ежедневных пределов.

Планирование площадок

Ознакомьтесь с вариантами использования и оцените факторы, чтобы обеспечивать наиболее эффективную защиту данных для дискового решения с несколькими площадками на основе IBM Spectrum Protect.

Случаи использования

Дисковое решение с несколькими площадками создает, как минимум, одну копию данных резервных копий. Если серверы IBM Spectrum Protect находятся в разных расположениях, резервная копия реплики хранится вне площадки.
Совет: Избегайте конфликтов при управлении административными ID и наборами опций клиентов, выявляя ID и наборы опций, реплицированные на сервер назначения, и ID и наборы опций, управление которыми будет осуществляться в конфигурации предприятия. Вы не сможете задать ID административного пользователя для зарегистрированного узла, если для этого узла существует административный ID.
Хотя и могут быть разные причины, по которым ваша компания могла бы получить преимущество от дискового решения с несколькими площадками, наиболее общие причины использования дискового решения с несколькими площадками включают в себя следующие сценарии репликации:

Репликация из первичной площадки на площадку аварийного восстановления данных

В этом сценарии данные, резервная копия которых создается с первичной площадки A, реплицируются на сервер на вторичной площадке аварийного восстановления, площадке B. Если на площадке A произойдет авария, например, сбой сервера, вы сможете использовать сервер на площадке B для восстановления системы. Либо можно использовать сервер на площадке A, чтобы восстановить данные первичного пула хранения на площадке B, например, после ошибки дискового хранилища на площадке B.

Взаимная репликация на двух активных площадках

В этом сценарии производится резервное копирование локальных данных на каждой площадке серверами на площадке A и площадке B. Данные, резервная копия которых создавалась с площадки A, реплицируются на площадку B, а резервные копии данных с площадки B реплицируются на площадку A. Если данные, для которых была создана резервная копия, окажутся потеряны на площадке A, вы сможете использовать сервер на площадке B, чтобы восстановить данные пула хранения на сервер на площадке A. Если площадка A станет недоступна, вы сможете восстановить реплицированные данные для площадки A в новую систему на площадке B. Вы должны подобрать размер ресурсов сервера так, чтобы убедиться, что на любом сервере в вашем плане аварийного восстановления есть достаточно мощностей для резервного копирования и восстановления всех клиентских узлов.

Защитите удаленные серверы на первичной площадке

В этом сценарии вы конфигурируете удаленные серверы, которые относительно малы для репликации данных, резервные копии которых создаются на более крупном сервере на первичной площадке. Если полоса пропускания ограничена, восстановление систем на удаленных площадках может оказаться нецелесообразным. В этом случае разумным шагом с вашей стороны было бы восстановить системы на первичной площадке, прежде чем реплицировать резервные копии данных на удаленные серверы.

Факторы для оценки

Прежде чем реализовать дисковое решение с несколькими площадками, оцените следующие факторы:

Пропускная способность сети

У сети должна быть достаточная пропускная способность, соответствующая ожидаемой передаче данных между узлами при репликации и при выполнении операций восстановления с одной площадки на другую, если это требуется для аварийного восстановления. Прежде чем приступать к тестированию пропускной способности

репликации, убедитесь, что сеть способна обработать трафик репликации. Вычислите необходимую пропускную способность сети в соответствии с требованиями стабильного состояния, используя рекомендации в разделе Оценка пропускной способности сети, необходимой для репликации (V7.1.1).

Сетевое соединение часть является совместно используемым ресурсом. Запланируйте запуск расписания репликации узла на такое время суток, чтобы избежать конфликта с другими пользователями ресурсов. Также можно использовать элементы управления сетью, чтобы ограничить операции только частью полосы пропускания. В IBM Spectrum Protect нет никаких элементов управления, которые бы позволяли ограничить использование сети.

Ресурсы для начальной репликации

Чтобы настроить решение по защите данных на двух площадках, нужно сначала реплицировать данные с площадки A на целевой сервер на площадке B. Чтобы первоначальная репликация прошла успешно, нужно определить, достаточно ли для нее пропускной способности сети, процессорных ресурсов и времени. Возможно, вам придется запланировать репликацию первоначальных полных резервных копий в течение нескольких дней. Если вы не можете распространить расписание на первоначальные резервные копии, вы можете реплицировать данные с площадки A на площадку B, не используя сеть. Например, можно экспортировать и импортировать резервные копии данных, используя носители, или можно временно поместить исходный и целевой серверы на одну и ту же площадку.

Ежедневный ввод данных

В случае дискового решения с несколькими площадками ежедневный ввод данных и общее хранение даных должны находиться в пределах емкости конфигураций. Например, в крупной конфигурации есть емкость для ввода данных, достигающая 100 ТБ в день, включая репликацию узлов. В тех случаях, когда требования к резервному копированию превышают емкость одного сервера, можно сконфигурировать решение, использующее несколько серверов, которые обеспечат нужную емкость.

Конфигурация сервера

Конфигурация сервера должна соответствовать требованиям к дисковому решению с несколькими площадками или должна превосходить эти требования.

Одна реплика резервных копий данных

Дисковое решение с несколькими площадками наиболее эффективно, если одна внесайтовая резервная копия данных соответствует вашим требованиям к защите данных и профилактике рисков. В этом случае одна резервная копия данных остается вне площадки в расположении сервера репликации.

Ссылки, связанные с данной:
Требования к системе для дискового решения с несколькими площадками

Требования к системе для дискового решения с несколькими площадками

После выбора решения IBM Spectrum Protect, наилучшим образом соответствующего вашим требованиям к защите данных, ознакомьтесь с требованиями к системе, чтобы спланировать реализацию решения по защите данных.

Убедитесь, что система соответствует требованиям к аппаратным и программным средствам для сервера того размера, который вы собираетесь использовать.

- Требования к аппаратным средствам
  Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.
- Требования к программному обеспечению
  Документация для дискового решения IBM Spectrum Protect с несколькими площадками содержит задачи по установке и конфигурированию для указанных ниже операционных систем. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информация, связанная с данной:
Поддерживаемые операционные системы для IBM Spectrum Protect

Требования к аппаратным средствам

Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.

Определение системных размеров можно найти в t_msdisk_select_size.html.

В следующей таблице перечислены минимальные требования к аппаратному обеспечению сервера и хранилища на основе размера сервера, который вы собираетесь построить. Если вы используете локальные разделы (LPAR) или рабочие разделы (WPAR), скорректируйте требования к сети, чтобы учесть размер разделов.

В качестве отправной точки используйте информацию, содержащуюся в следующей таблице. Самую свежую информацию о требованиях к оборудованию и спецификациях для сервера и хранилища смотрите в разделе IBM Spectrum Protect Blueprints.

Аппаратный компонент	**Небольшая система**	**Средняя система**	**Крупная система**
Процессор сервера	 Операционные системы AIX 6 ядер процессора, 3,42 ГГц или быстрее  Операционные системы Linux  Операционные системы Windows 16 ядер процессора, 1,7 ГГц или быстрее	 Операционные системы AIX 10 ядер процессора, 3,42 ГГц или быстрее  Операционные системы Linux  Операционные системы Windows 20 ядер процессора, 2,2 ГГц или быстрее	 Операционные системы AIX 20 ядер процессора, 3,42 ГГц  Операционные системы Linux  Операционные системы Windows 44 ядра процессора, 2,2 ГГц или быстрее
Память сервера	64 ГБ ОП	128 ГБ ОП	256 ГБ ОП
Сеть	• 10 ГБ Ethernet (1 порт) • Адаптер 8 ГБ Fibre Channel (2 порта)	• 10 ГБ Ethernet (2 порта) • Адаптер 8 ГБ Fibre Channel (2 порта)	• 10 ГБ Ethernet (4 порта) • Адаптер 8 ГБ Fibre Channel (4 порта)
Хранение	• Диски SSD 1,45 Тб для базы данных, плюс пространство для записей Центр операций • 67 ТБ пула хранения каталогов-контейнеров с дедупликацией	• Диски SSD 2,53 Тб для базы данных, плюс пространство для записей Центр операций • 207,9 ТБ пула хранения каталогов-контейнеров с дедупликацией	• Диски SSD 6,54 Тб для базы данных, плюс пространство для записей Центр операций • 1049,67 ТБ пула хранения каталогов-контейнеров с дедупликацией

Реализация правильной технологии ядра процессора

Надо использовать правильный тип технологии ядра процессора для процессора сервера. Информацию о типе базовой технологии процессора смотрите в разделе IBM Spectrum Protect Blueprints.

Оценка необходимого объема пространства для базы данных Центр операций

Требования к аппаратным средствам для Центр операций включены в предыдущую таблицу за исключением пространства базы данных и архивного журнала (перечня), которые используются компонентом Центр операций для удерживания записей для управляемых клиентов.

Если вы не собираетесь устанавливать Центр операций на том же компьютере, что и сервер, вы можете оценить требования к системе отдельно. Чтобы вычислить требования к системе для компонента Центр операций, смотрите описание калькулятора требований к системе в документе техническое замечание 1641684.

Управление компонентом Центр операций на сервере - это рабочая нагрузка, требующая дополнительного пространства для операций базы данных. Объем пространства зависит от числа клиентов, мониторинг которых осуществляется на сервере. Прочтите следующие рекомендации, которые позволяют оценить, какой объем пространства потребуется вашему серверу.

Пространство базы данных

Компонент Центр операций использует, примерно, 1,2 ГБ пространства базы данных на каждую 1000 клиентов, отслеживаемых на сервере. Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1500 клиентов. Эта конфигурация дает в итоге 6500 клиентов на четырех серверах, и для нее требуется примерно 8,4 ГБ пространства базы данных. Это значение вычисляется путем округления 6500 клиентов до следующей ближайшей 1000, что составит 7000:

```
7 x 1,2 ГБ=8,4 ГБ
```

Пространство архивного журнала

Центр операций использует, примерно, 8 ГБ пространства архивного журнала каждые 24 часа для каждой 1000 клиентов. В примере 6500 клиентов работают через хаб-серверы и подчиненные сервера, и за 24 часа для хаб-сервера используется 56 ГБ пространства архивного журнала.
Для каждого подчиненного сервера в примере пространство архивного журнала, используемое в течение 24 часов, составит около 16 ГБ. Эти оценки основаны на интервале сбора данных о состоянии по умолчанию, равном 5 минутам. Если вы сократите интервал сбора данных с одного раза за 5 минут до одного раза за 3 минуты, требования к пространству возрастут. В следующих примерах показано примерное увеличение требований к пространству журнала при интервале сбора данных один раз в 3 минуты:

- Хаб-сервер: С 56 ГБ примерно до 94 ГБ
- Каждый подчиненный сервер: С 16 ГБ примерно до 28 ГБ

Увеличьте пространство архивного журнала так, чтобы у вас было достаточно доступного пространства для поддержки компонента Центр операций и чтобы это не влияло на существующие операции сервера.

Требования к аппаратному обеспечению второго сервера

Если вы собираетесь настроить свои площадки так, чтобы все на первой площадке реплицировалось на вторую площадку, требования к аппаратным средствам будут идентичны на обоих площадках. Если вы хотите реплицировать на вторую площадку только подмножество данных, требования к хранению и сети могут быть снижены.

Требования к программному обеспечению

Документация для дискового решения IBM Spectrum Protect с несколькими площадками содержит задачи по установке и конфигурированию для указанных ниже операционных систем. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информацию о требованиях к программам для драйверов устройств IBM® lin_tape смотрите в разделе Руководство по установке и использованию IBM Tape Device Drivers.

Системы AIX

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	IBM AIX 7.1 Дополнительную информацию о требованиях к операционным системам смотрите в разделе AIX: инимальные требования к системе для систем AIX.
Утилита gunzip	Утилита gunzip должна быть доступна в вашей системе до установки или обновления сервера IBM Spectrum Protect. Убедитесь, что утилита gunzip установлена и ее путь задан в переменной среды PATH.

Тип ПО	Минимальные требования к программному обеспечению
Тип файловой системы	Файловые системы JFS2 Системы AIX могут кэшировать большие объемы данных файловой системы; при этом может сокращаться объем памяти, необходимый серверу и процессам IBM DB2. Чтобы избежать подкачки при использовании сервера AIX, используйте для файловой системы JFS2 опцию монтирования rbrw. Для кэша файловой системы используется меньше памяти, и для IBM Spectrum Protect будет доступно больше памяти. Не используйте опции монтирования файловой системы с параллельным вводом-выводом (Concurrent I/O, CIO) и с прямым вводом-выводом (Direct I/O, DIO) для файловых систем, содержащих журналы базы данных IBM Spectrum Protect или тома пулов хранения. Использование этих опций может вызывать снижение производительности многих серверных операций. IBM Spectrum Protect и DB2 все равно могут использовать DIO там, где это выгодно, но для IBM Spectrum Protect не требуются опции монтирования, чтобы выборочно использовать преимущества этого метода.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Linux

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Red Hat Enterprise Linux 7 (x86_64)
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, устанавливаемые в системе IBM Spectrum Protect. Серверы Red Hat Enterprise Linux: • libaio • libstdc++.so.6 (требуются 32- и 64-разрядные пакеты) • numactl.x86_64
Тип файловой системы	Сформатируйте файловые системы, связанные с базами данных, используя ext3 или ext4. Для файловых систем, связанных с пулами, используйте XFS.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Windows

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Microsoft Windows Server 2012 R2 (64-разрадная система) или Windows Server 2016
Тип файловой системы	NTFS
Другое программное обеспечение	Должны быть установлены и включены Windows 2012 R2 или Windows 2016 с платформой .NET Framework 3.5. Должны быть отключены следующие политики управления учетными записями пользователей: • Управление учетными записями пользователей: Режим Утверждать администраторов для встроенной учетной записи Администратор • Управление учетными записями пользователей: Запускать всех администраторов в режиме Утверждать администраторов

Задачи, связанные с данной:

Настройка сетевых опций AIX

Рабочие листы планирования

Используйте рабочие таблицы планирования, чтобы записывать в них значения, которые вы используете при настройке системы с последующим конфигурированием сервера IBM Spectrum Protect. Используйте наилучшие практические значения по умолчанию, приведенные в рабочих таблицах.

Каждая рабочая таблица поможет вам подготовиться к разным стадиям конфигурирования системы за счет использования наилучших практических значений:

Предварительное конфигурирование серверной системы
: Используйте рабочие таблицы предварительного конфигурирования для планирования файловых систем и каталогов, которые вы создадите, когда сконфигурируете файловые системы для IBM Spectrum Protect во время настройки системы. Все каталоги, созданные вами для сервера, должны быть пустыми.

Конфигурация сервера
: Воспользуйтесь рабочими таблицами по конфигурированию, когда будете конфигурировать сервер. Для большинства элементов предлагаются значения по умолчанию, кроме случаев, когда это отмечено.

AIX

Табл. 1. Рабочая таблица для предварительного конфигурирования серверной системы AIX

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	/home/tsminst1/tsminst1		50 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 2.
Каталог для установки сервера	/		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/usr		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/var		Доступное пространство, необходимое для каталога: 5 ГБ	
Каталог для установки сервера	/tmp		Доступное пространство, необходимое для каталога: 5 ГБ	

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталог для установки сервера	/opt		Доступное пространство, необходимое для каталога: 10 ГБ	
Каталог для активного журнала	/tsminst1/TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	Если вы создаете активный журнал при первоначальном конфигурировании сервера, задайте размер, равный 128 ГБ.
Каталог для архивного журнала	/tsminst1/TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	
Каталоги для базы данных	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем
Каталоги для хранения	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 2. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 1, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	passw0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра DB2	tsmsrvrs		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Linux

Табл. 3. Рабочая таблица для предварительного конфигурирования серверной системы Linux

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	/home/tsminst1/tsminst1		25 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 4.
Каталог для активного журнала	/tsminst1/TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	
Каталог для архивного журнала	/tsminst1/TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	
Каталоги для базы данных	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для хранения	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 4. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 3, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	passw0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра DB2	tsmsrvrs		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Windows

Поскольку много томов создается для сервера, сконфигурируйте сервер, используя имеющуюся в Windows функцию отображения дисковых томов в каталоги, а не в буквы дисков.

Например, C:\tsminst1\TSMdbpsace00 - это точка монтирования для тома с его собственным пространством. Том отображается в каталог на диске C:, но не занимает пространство на диске C:. Исключением является каталог экземпляра сервера, C:\tsminst1, который может быть точкой монтирования или обычным каталогом.

Табл. 5. Рабочая таблица для предварительного конфигурирования серверной системы Windows

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	C:\tsminst1		25 ГБ	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 6.
Каталог для активного журнала	C:\tsminst1\TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	
Каталог для архивного журнала	C:\tsminst1\TSMarchlog		• Небольшие: 1 ТБ • Средние: 2 ТБ • Крупные: 4 ТБ	
Каталоги для базы данных	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 1 ТБ • Средние: не менее 2 ТБ • Крупные: не менее 4 ТБ	Создайте минимальное число файловых систем для базы данных в зависимости от размера вашей системы: • Небольшие: не менее 4 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 8 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для хранения	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 38 ТБ • Средние: не менее 180 ТБ • Крупные: По крайней мере, 500 ТБ	Создайте минимальное число файловых систем для хранения в зависимости от размера вашей системы: • Небольшие: не менее 10 файловых систем • Средние: не менее 20 файловых систем • Крупные: не менее 40 файловых систем

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
Каталоги для резервного копирования базы данных	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		Минимальное общее пространство для всех каталогов: • Небольшие: не менее 3 ТБ • Средние: не менее 10 ТБ • Крупные: не менее 16 ТБ	Создайте минимальное число файловых систем для резервного копирования базы данных в зависимости от размера вашей системы: • Небольшие: не менее 2 файловых систем • Средние: не менее 4 файловых систем • Крупные: не менее 4 файловых систем, предпочтительно 6 Первый каталог резервных копий базы данных также используется как каталог отказоустойчивости журнала архивирования и как вторая копия хронологии тома и файлов конфигурации устройства.

Табл. 6. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Примечания
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 5, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	pAssW0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		

Элемент	Значение по умолчанию	Собственное значение	Примечания
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	22:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента.

Планирование хранения

Выберите наиболее эффективную технологию хранения для компонентов IBM Spectrum Protect, чтобы обеспечить эффективную работу сервера и высокую производительность операций.

У аппаратных устройств хранения разные характеристики емкости и производительности, что определяет то, как их можно эффективно использовать вместе с IBM Spectrum Protect. Общие рекомендации по выбору соответствующего оборудования хранения и настройке вашего решения смотрите в указанных ниже источниках.

База данных и активный журнал

- Используйте для базы данных и активного журнала IBM Spectrum Protect быстрый диск, например, со следующими характеристиками:
  - Высокопроизводительный диск 15 K rpm с оптоволоконным (Fibre Channel) или последовательно подключенным интерфейсом SCSI (SAS).
  - Твердотельный диск (Solid-state disk, SSD)

- Изолируйте активный журнал от базы данных, если вы не используете твердотельное (SSD) или флеш-оборудование
- При создании массивов для базы данных используйте RAID уровня 5

Пул хранения

- Для пула хранения можно использовать менее дорогие и более медленные диски
- Пул хранения данных может совместно использовать диски для хранения архивного журнала и резервной копии базы данных
- Используйте RAID уровня 6 для массивов пулов хранения, чтобы добавить защиту от двойных сбоев диска при использовании крупных типов дисков

- Планирование массивов хранения
  Подготовьтесь к конфигурированию дискового хранения, спланировав массивы RAID и тома в соответствии с размером вашей системы IBM Spectrum Protect.

Ссылки, связанные с данной:
Требования к системе хранения и уменьшение риска повреждения данных

Планирование защиты

Спланируйте защиту систем в решении IBM Spectrum Protect, используя управление доступом и аутентификацией, и рассмотрите возможность шифрования данных и передачи паролей.

Рекомендации относительно защиты вашей среды хранения от атак программ, требующих выкуп, и восстановления среды хранения, если произойдет атака, смотрите в разделе Защита среды хранения против программ-вымогателей.

- Планирование ролей администратора
  Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.
- Планирование защищенной связи
  План защиты взаимодействий между компонентами решения IBM Spectrum Protect.
- Планирование хранения зашифрованных данных
  Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите возможности, которые лучше всего подходят для ваших требований.
- Планирование доступа через брандмауэр
  Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

Планирование ролей администратора

Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.

Администраторам можно назначить один из следующих уровней полномочий:

Система
: У администраторов с системными полномочиями - высший уровень полномочий. Администраторы с этим уровнем полномочий могут выполнить любую задачу. Они могут управлять всеми доменами политики и пулами хранения и предоставлять полномочия другим администраторам.

Политика
: Администраторы, у которых есть полномочия политики, могут управлять всеми задачами, связанными с управлением политикой. Эти полномочия могут быть неограниченными или могут быть ограничены определенными доменами политики.

Хранение
: Администраторы, у которых есть полномочия хранения, могут выделить ресурсы хранения для сервера и управлять ими.

Оператор
: Администраторы, у которых есть полномочия оператора, могут управлять непосредственной работой сервера и доступностью таких носителей хранения, как ленточные библиотеки и накопители.

В сценариях в Табл. 1 представлены примеры того, почему вам может потребоваться назначить разные уровни полномочий, чтобы администраторы могли выполнять задачи:

Табл. 1. Сценарии для ролей администраторов

Сценарий	Тип ID администратора, который нужно задать
Администратор в небольшой компании управляет сервером и отвечает за все операции сервера.	• Системные полномочия: 1 ID администратора
Администратор нескольких серверов также управляет всей системой. Несколько других администраторов управляют своими собственными пулами хранения.	• Системные полномочия на всех серверах: 1 ID администратора для всех задач по администрированию системы • Полномочия на хранение для назначенных пулов хранения: 1 ID администратора для каждого из других администраторов
Администратор управляет двумя серверами. Другой сотрудник помогает выполнять задачи по администрированию. Два помощника отвечают за то, чтобы производилось резервное копирование важных систем. Каждый помощник отвечает за мониторинг запланированных операций по резервному копированию на одном из серверов IBM Spectrum Protect.	• Системные полномочия на обоих серверах: 2 ID администратора • Полномочия оператора: 2 ID администраторов для помощников с доступом к серверу, за который отвечает каждый сотрудник

Планирование защищенной связи

План защиты взаимодействий между компонентами решения IBM Spectrum Protect.

Определите уровень защиты, требующийся для ваших данных, на основе нормативов и бизнес-требований, которые действуют в вашей компании.

Если для вашего бизнеса требуется высокий уровень защиты паролей и передаваемых данных, запланируйте реализацию защищенной связи на основе протоколов Transport Layer Security (TLS) или Secure Sockets Layer (SSL).

TLS и SSL обеспечивают защищенную связь между сервером и клиентом, но могут отрицательно влиять на производительность системы. Чтобы повысить производительность системы, используйте TLS для аутентификации без шифрования данных объектов. Чтобы указать, использует ли сервер TLS 1.2 для всего сеанса или только для аутентификации, смотрите описание опции клиента SSL для взаимодействий клиента с сервером и параметра UPDATE SERVER=SSL для взаимодействий сервера с сервером. Beginning in V8.1.2, TLS is used for authentication by default. Если вы решите использовать TLS для шифрования всего сеанса, используйте этот протокол только для сеансов, в которых это необходимо, и добавьте на сервер процессорные ресурсы, чтобы справиться с увеличением сетевого трафика. Также можно попробовать использовать другие опции. Например, в некоторых сетевых устройствах, например, в маршрутизаторах и коммутаторах, есть функция TLS или SSL.

TLS и SSL можно использовать для защиты некоторых или всех различных возможных путей связи, например:

- Центр операций: браузер с хабом; хаб с подчиненным сервером
- Клиент с сервером
- Сервер с сервером: репликация узлов

Задачи, связанные с данной:
Защита связи

Планирование хранения зашифрованных данных

Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите возможности, которые лучше всего подходят для ваших требований.

Если вашей компания требуется шифровать данные в пулах хранения, вы можете использовать шифрование IBM Spectrum Protect или такое внешнее устройство, как лента для шифрования.

Если вы выбираете IBM Spectrum Protect для шифрования данных, на клиенте потребуются дополнительные вычислительные ресурсы, что может повлиять на производительность процессов резервного копирования и восстановления.

Информация, связанная с данной:
technote 1963635

Планирование доступа через брандмауэр

Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

В разделе Табл. 1 описаны порты, используемые сервером, клиентом и компонентом Центр операций.

Табл. 1. Порты, используемые сервером, клиентом и компонентом Центр операций

Элемент	По умолчанию	Направление	Описание
Базовый порт (TCPPORT)	1500	Исходящие/ входящие	Для каждого экземпляра сервера требуется уникальный порт. Вместо порта по умолчанию можно задать альтернативный номер порта. Опция TCPPORT принимает от клиента как сеансы TCP/IP, так и сеансы с поддержкой SSL. Для трафика клиента администрирования можно задать значения портов, используя опции TCPADMINPORT и ADMINONCLIENTPORT.
SSL-only port (SSLTCPPORT)	Значения по умолчанию нет	Исходящие/ входящие	Этот порт используется, если вы хотите ограничить взаимодействия на порту только сеансами, поддерживающими SSL. Чтобы обеспечить поддержку взаимодействий как SSL, так и не SSL, используйте опции TCPPORT или TCPADMINPORT.
SMB	45	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SSH	22	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SMTP	25	Исходящие	Этот порт используется для отправки оповещений с сервера по электронной почте.
NDMP	Значения по умолчанию нет	Входящие/ исходящие	Сервер должен иметь возможность открыть соединение исходящего управляющего порта NDMP с устройством NAS. Исходящий управляющий порт - это низкоуровневый адрес в определении функции перемещения данных для устройства NAS. При восстановлении с файл-сервера NDMP на сервер сервер должен иметь возможность открыть соединение исходящего соединения данных NDMP с устройством NAS. Порт соединения данных, который используется при восстановлении, можно сконфигурировать на устройстве NAS. При создании резервных копий с файл-сервера NDMP на сервер устройство NAS должно иметь возможность открыть исходящие соединения данных с сервером, а сервер должен быть способен принять входящие соединения данных NDMP. При помощи серверной опции NDMPPORTRANGE можно ограничить набор портов, доступных для использования в качестве соединений данных NDMP. Вы можете сконфигурировать брандмауэр для соединения с этими портами.
Репликация	Значения по умолчанию нет	Исходящие/ входящие	Порт и протокол для исходящего порта при репликации заданы командой DEFINE SERVER, которая используется, чтобы настроить репликацию. Входящие порты для репликации - это порты TCP и порты SSL, которые исходный сервер указывает в команде DEFINE SERVER.

Элемент	По умолчанию	Направление	Описание
Порт клиентских расписаний	Порт клиента: 1501	Исходящие	Клиент осуществляет прием на указанном порту и передает номер порта серверу. Сервер соединяется с клиентом, если используется планирование по приглашению сервера. Можно задать альтернативный номер порта в файле опций клиента.
Длительно выполн. сеансы	Параметр KEEPALIVE: YES	Исходящие	Если включена опция KEEPALIVE, пакеты проверки активности (keepalive) отправляются во время сеансов клиент-сервер, чтобы не дать программе брандмауэра закрыть длительно выполняющиеся, неактивные соединения.
Центр операций	HTTPS: 11090	Входящие	Эти порты используются для веб-браузера компонента Центр операций. Можно задать альтернативный номер порта.
Порт службы управления клиентами	Порт клиента: 9028	Входящие	Порт службы управления клиентами должен быть доступен из компонента Центр операций. Убедитесь, что брандмауэры не запрещают соединения. Служба управления клиентами использует порт TCP сервера клиентского узла для аутентификации, используя административный сеанс.

Реализация решения по защите данных на диске для нескольких площадок

Дисковое решение с несколькими площадками конфигурируется на двух площадках и использует дедупликацию данных и репликацию.

Путеводитель по реализации

Описанные ниже шаги необходимы, чтобы настроить дисковую среду с несколькими площадками.

1. Настройте систему.
    a. Сконфигурируйте аппаратуру хранилища и настройте массивы хранения, соответствующие размеру вашей среды.
    b. Установите операционную систему сервера.
    c. Сконфигурируйте ввод-вывод с несколькими путями.
    d. Создайте ID пользователя для экземпляра сервера.
    e. Подготовьте файловые системы для IBM Spectrum Protect.
2. Установите сервер и Центр операций.
3. Сконфигурируйте сервер и Центр операций.
    a. Выполните первоначальное конфигурирование сервера.
    b. Задайте опции сервера.
    c. Сконфигурируйте SSL (Secure Sockets Layer) для сервера и клиента.
    d. Сконфигурируйте Центр операций.
    e. Зарегистрируйте свою лицензию на IBM Spectrum Protect.
    f. Настройте дедупликацию данных.
    g. Задайте правила хранения данных для вашего бизнеса.
    h. Задайте расписания обслуживания сервера.
    i. Задайте расписания клиентов.
4. Установите и сконфигурируйте клиенты.
    a. Зарегистрируйте клиенты и назначьте их для расписаний.
    Совет: Избегайте конфликтов при управлении административными ID и наборами опций клиентов, выявляя ID и наборы опций, реплицированные на сервер назначения, и ID и наборы опций, управление которыми будет осуществляться в конфигурации предприятия. Вы не сможете задать ID административного пользователя для зарегистрированного узла, если для этого узла существует административный ID.
    b. Установите и проверьте службу управления клиентом.
    c. Сконфигурируйте Центр операций на использование службы управления клиентом.
5. Сконфигурируйте второй сервер.
    a. Сконфигурируйте связь SSL между хаб-сервером и подчиненным сервером.
    b. Добавьте второй сервер как подчиненный сервер.
    c. Включите репликацию.

6. Завершите реализацию.

Настройка системы

Чтобы настроить систему, нужно сначала сконфигурировать дисковое оборудование хранения и серверную систему для IBM Spectrum Protect.

- Конфигурирование оборудования систем хранения
  Чтобы сконфигурировать оборудование систем хранения, прочтите общие рекомендации по дисковым системам и IBM Spectrum Protect.
- Установка операционной системы сервера
  Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.
- Конфигурирование ввода-вывода с несколькими путями
  Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.
- Создание ID пользователя для сервера
  Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.
- Подготовка файловых систем для сервера
  Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

Конфигурирование оборудования систем хранения

Чтобы сконфигурировать оборудование систем хранения, прочтите общие рекомендации по дисковым системам и IBM Spectrum Protect.

Процедура

1. Задайте соединение между сервером и устройствами хранения, следуя приведенным ниже рекомендациям:
   - Используйте коммутируемое или прямое усоединение для соединений Fibre Channel.
   - Подберите число портов для соединения и учетную запись для необходимой ширины полосы пропускания.
   - Подберите число портов для соединения на сервере и число портов хоста в дисковой системе.
2. Убедитесь, что драйверы устройств и встроенная микропрограмма в системе сервера, адаптеров и операционной системы, являются современными и находятся на рекомендуемых уровнях.
3. Сконфигурируйте массивы хранения. Убедитесь, что вы правильно произвели планирование, чтобы обеспечить оптимальную производительность. Дополнительную информацию смотрите в разделе Планирование хранения.
4. Убедитесь, что у системы сервера есть доступ к созданным дисковым томам. Сделайте следующее:
   a. Если система подключена к коммутатору Fibre Channel, произведите зонирование сервера, чтобы увидеть диски.
   b. Отобразите все тома, чтобы сообщить дисковой системе, что данному серверу разрешено видеть каждый диск.

Задачи, связанные с данной:
Конфигурирование хранения

Установка операционной системы сервера

Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.

- Установка в системах AIX
  Выполните следующие действия, чтобы установить AIX в системе сервера.
- Установка в системах Linux
  Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.
- Установка в системах Windows
  Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Установка в системах AIX

Выполните следующие действия, чтобы установить AIX в системе сервера.

Процедура

1. Установите AIX версии 7.1 TL4, SP2 или новее в соответствии с инструкциями производителя.
2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

     ```
     127.0.0.1 localhost
     ```

4. Включите полты выполнения ввода-вывода AIX, введя следующую команду:

   ```
   chdev -l iocp0 -P
   ```

   На производительность сервера может влиять определение часового пояса по Олсону (Olson).
5. Чтобы оптимизировать производительность, измените формат часового пояса с Olson на POSIX. Чтобы обновить параметр часового пояса, используйте следующий формат команды:

   ```
   chtz=локальный_часовой_пояс,дата/время,дата/время
   ```

   Например, если вы находитесь в Тьюсоне (Аризона), где используется стандартное горное время, то вы бы, чтобы перейти к формату POSIX, ввели бы следующую команду:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Добавьте запись в файл .profile пользователя экземпляра, чтобы была задана следующая среда:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Совет: Если пользователь экземпляра недоступен, то выполните этот шаг позже, когда пользователь экземпляра станет доступен.
7. Настройте систему на создание полных файлов ядра приложения. Введите следующую команду:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Чтобы обеспечить взаимодействия с сервером и компонентом Центр операций, убедитесь, что на всех брандмауэрах, которые могут существовать, открыты следующие порты:
   - Для связи с сервером откройте порт 1500.
   - Чтобы обеспечить защищенную связь с компонентом Центр операций, откройте порт 11090 на хаб-сервере.

   Если вы не используете значения портов по умолчанию, то убедитесь, что используемые вами порты открыты.

9. Включите усовершенствования высокой производительности TCP. Введите следующую команду:

   ```
   no -p -o rfc1323=1
   ```

10. Чтобы обеспечить оптимальную пропускную способность и надежность, свяжите вместе четыре порта 10 Gb Ethernet. Используйте инструмент System Management Interface Tool (SMIT), чтобы связать порты друг с другом, используя Etherchannel. При тестировании использовались следующие параметры:

    ```
    режим            8023ad
    auto_recovery    yes             Включить автоматическое восстановление после
                                     передачи управления
    backup_adapter   NONE            Адаптер, используемый при ошибке всего канала
    hash_mode        src_dst_port    Указывает, как выбирается исходящий адаптер
    interval         long            Определяет значение интервала для режима
                                     IEEE 802.3ad
    mode             8023ad          Режим EtherChannel для операции
    netaddr          0               Адрес для команды ping
    noloss_failover  yes             Включает передачу управления без потери данных
                                     после неудачного завершения ping
    num_retries      3               Сколько раз повторять ping, прежде чем заключить
    ```

```
                                о неудаче
retry_time      1               Время ожидания (в сек.) между командами ping
use_alt_addr    no              Включить другой адрес EtherChannel
use_jumbo_frame no              Включить фреймы Gigabit Ethernet Jumbo
```

11. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 1. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 1. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	**Установка**	**Значение**	**Команда для запроса значения**
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Linux

Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.

Прежде чем начать

Операционная система устанавливается на внутренних жестких дисках. Сконфигурируйте внутренние жесткие диски, используя аппаратный массив RAID 1. Например, если вы конфигурируете небольшую систему, два внутренних диска по 300 ГБ зеркально отражаются в RAID 1, в результате чего для программы установки операционной системы будет доступен один диск в 300 ГБ.

Процедура

1. Установите Red Hat Enterprise Linux версии 7.1 или новее в соответствии с инструкциями производителя. Получите загрузочный DVD-диск, содержащий Red Hat Enterprise Linux версии 7.1 и запустите свою систему с этого DVD-диска. Опции установки смотрите в приведенных ниже рекомендациях. Если элемент не упомянут в приведенном ниже списке, оставьте для него значение по умолчанию.
    a. После запуска DVD-диска выберите в меню Установить или обновить существующую систему.
    b. В окне с приветствием выберите Проверить этот носитель и установить Red Hat Enterprise Linux 7.1.
    c. Выберите предпочтения языка и клавиатуры.
    d. Выберите свое расположение, чтобы задать нужный часовой пояс.
    e. Выберите Выбор программ, а затем в следующем окне выберите Сервер с графическим пользовательским интерфейсом.
    f. На странице сводной информации установки щелкните по Пункт назначения установки и проверьте следующее:
        - В качестве пункта назначения установки выбирается локальный диск на 300 ГБ.
        - В разделе Другие опции хранения выбирается опция Автоматически сконфигурировать разбиение на разделы.

    Щелкните по Готово.
    g. Щелкните по Начать установку . После запуска установки задайте пароль пользователя root для учетной записи пользователя root.

По завершении установки перезапустите систему и войдите в систему от имени пользователя root. Введите команду df, чтобы проверить базовое разбиение на разделы. Например, в тест-системе первоначальные разделы выдали следующий результат:

```
[root@tvapp02]# df -h
Файловая сист.                  Размер Исп. Дост. Исп. % Где смонтир.
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G    1%    /dev/shm
tmpfs                   32G   8.8M  32G    1%    /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
   Чтобы обеспечить оптимальную пропускную способность и надежность, рассмотрите возможность связать вместе несколько сетевых портов. Это можно выполнить, создав сетевое соединение Link Aggregation Control Protocol (LACP), которое агрегирует несколько подчиненных портов в одно логическое соединение. Предпочтительный метод состоит в том, чтобы использовать режим связи 802.3ad, параметр miimon, равный 100, и параметр xmit_hash_policy, равный layer3+4.
   Ограничение: Для использования сетевого соединения LACP у вас должен быть сетевой коммутатор, поддерживающий LACP.

   Дополнительные инструкции по конфигурированию привязанных сетевых соединения при использовании Red Hat Enterprise Linux версии 7 смотрите в документе: Создать интерфейс привязки каналов.

3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

     ```
     127.0.0.1 localhost
     ```

4. Установите компоненты, необходимые для установки сервера. Выполните описанные ниже шаги, чтобы создать репозиторий Yellowdog Updater Modified (YUM) и установить необходимые пакеты.
   a. Смонтируйте DVD-диск установки Red Hat Enterprise Linux в системном каталоге. Например, чтобы смонтировать его в каталоге /mnt, введите следующую команду:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Убедитесь, что DVD-диск смонтирован, введя команду mount. Должна появиться выходная информация, аналогичная следующему примеру:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Перейдите в каталог репозитория YUM, введя следующую команду:

      ```
      cd /etc/yum/repos.d
      ```

      Если каталог repos.d не существует, создайте его.
   d. Вызовите список содержимого каталога:

      ```
      ls rhel-source.repo
      ```

   e. Переименуйте исходный файл repo, введя команду mv. Например:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Создайте новый файл repo, используя текстовый редактор. Например, чтобы использовать редактор vi, введите следующую команду:

      ```
      vi rhel71_dvd.repo
      ```

   g. Добавьте в новый файл repo следующие строки. Параметр baseurl задает точку монтирования каталога:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      ```

```
enabled=1
gpgcheck=0
```

h. Установите необходимый пакет ksh.x86_64, введя команду yum. Например:

```
yum install ksh.x86_64
```

Исключительная ситуация: Устанавливать библиотеки compat-libstdc++-33-3.2.3-69.el6.i686 и libstdc++.i686 для Red Hat Enterprise Linux версии 7.1 не нужно.

5. По завершении установки программы вы сможете восстановить исходные значения репозитория YUM, выполнив следующие шаги:
   a. Размонтируйте DVD-диск установки Red Hat Enterprise Linux, введя следующую команду:

   ```
   unmount /mnt
   ```

   b. Перейдите в каталог репозитория YUM, введя следующую команду:

   ```
   cd /etc/yum/repos.d
   ```

   c. Переименуйте созданный вами файл repo:

   ```
   mv rhel71_dvd.repo rhel71_dvd.repo.orig
   ```

   d. Переименуйте исходный файл, используя его исходное имя:

   ```
   mv rhel-source.repo.orig rhel-source.repo
   ```

6. Определите, требуется ли измерения параметров ядра. Сделайте следующее:
   a. Используйте команду sysctl -a, чтобы вывести список значений параметров.
   b. Проанализируйте результаты, следуя рекомендациям в разделе Табл. 1, чтобы определить, не требуются ли какие-либо изменения.
   c. Если требуются изменения, задайте параметры в файле /etc/sysctl.conf. Изменения файлов применяются при запуске системы.

Совет: Автоматически корректируйте значения параметров ядра и устраните необходимость обновления этих параметров вручную. В Linux продукт программное обеспечение баз данных DB2 автоматически корректирует значения параметров ядра взаимодействий между процессами (interprocess communication, IPC) до предпочтительных значений. Чтобы получить дополнительную информацию о значениях параметров ядра, ищите параметры ядра Linux в публикации Документация по продукту DB2 версии 11.1 IBM.

Табл. 1. Оптимальные значения параметра ядра Linux

Параметр	**Описание**
kernel.shmmni	Максимальное число сегментов.
kernel.shmmax	Максимальный размер сегмента совместно используемой памяти (в байтах). Этот параметр нужно задать до автоматического запуска сервера IBM Spectrum Protect при запуске системы.
kernel.shmall	Максимальное число размещенных страниц совместно используемой памяти.
kernel.sem Существует четыре значения для параметра kernel.sem.	(SEMMSL) Максимальное число семафоров на массив.
	(SEMMNS) Максимальное число семафоров на систему.
	(SEMOPM) Максимальное число операций на вызов семафора.
	(SEMMNI) Максимальное число массивов.
kernel.msgmni	Максимальное число очередей сообщений уровня системы.

Параметр	Описание
kernel.msgmax	Максимальный размер сообщения (в байтах).
kernel.msgmnb	Максимальный размер очереди по умолчанию (в байтах).
kernel.randomize_va_space	Параметр kernel.randomize_va_space конфигурирует использование памяти ASLR для ядра. Отключите ASLR, так как это может вызвать ошибки в программе DB2. Дополнительные подробности об ASLR Linux и DB2 смотрите в документе техническое замечание 1365583.
vm.swappiness	Параметр vm.swappiness определяет, может ли ядро выполнять своппинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.
vm.overcommit_memory	Параметр vm.overcommit_memory влияет на то, какой объем виртуальной памяти ядро разрешает выделить. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.

7. Откройте порты брандмауэра для взаимодействия с сервером. Сделайте следующее:
   a. Определите зону, используемую сетевым интерфейсом. По умолчанию, это общедоступная зона.
      Введите следующую команду:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Чтобы использовать адрес порта по умолчанию для взаимодействия с сервером, откройте порт TCP/IP 1500 на брандмауэре Linux.
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Если вы хотите использовать какое-либо значение, отличающееся от значения по умолчанию, вы можете задать число в диапазоне 1024-32767. Если вы откроете порт, отличающийся от порта по умолчанию, вы должны будете указать порт при запуске сценария конфигурирования.

   c. Если вы собираетесь использовать эту систему как хаб, откройте порт 11090, который является портом по умолчанию для защищенных взаимодействий (https).
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Чтобы изменения вступили в силу, заново загрузите определения брандмауэра.
      Введите следующую команду:

      ```
      firewall-cmd --reload
      ```

8. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 2. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 2. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Windows

Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Процедура

1. Установите Windows Server 2016 Standard Edition, согласно инструкциям изготовителя.
2. Измените политики управления учетными записями Windows, выполнив следующие шаги:
   a. Откройте редактор локальной политики защиты, выполнив secpol.msc.
   b. Выберите Локальные политики > Опции защиты и убедитесь, что отключены следующие политики управления учетными записями пользователей:
      - Режим Утверждать администраторов для встроенной учетной записи Администратор
      - Запускать всех администраторов в режиме Утверждать администраторов
3. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
4. Примените обновления Windows и включите дополнительные функции, выполнив следующие шаги:
   a. Примените последние обновления Windows Server 2016.
   b. Установите и включите функцию Windows 2012 R2 Microsoft .NET Framework 3.5 при помощи менеджера сервера Windows.
   c. Если потребуется, обновите драйверы устройств FC и Ethernet HBA до новых уровней.
   d. Установите драйвер ввода-вывода с несколькими путями, соответствующий используемой вами дисковой системе.
5. Откройте порт TCP/IP по умолчанию, 1500, для связи с сервером IBM Spectrum Protect. Например, введите следующую команду:

   ```
   netsh advfirewall firewall add rule name="Backup server port 1500"
   dir=in action=allow protocol=TCP localport=1500
   ```

6. На хаб-сервере Центр операций откройте порт по умолчанию для защищенной (https) связи с компонентом Центр операций. Номер порта - 11090. Например, введите следующую команду:

   ```
   netsh advfirewall firewall add rule name="Центр операций port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Конфигурирование ввода-вывода с несколькими путями

Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.

- Системы AIX
- Системы Linux
- Системы Windows

Системы AIX

Процедура

1. Определите адрес порта Fibre Channel, который нужно использовать для определения хоста в дисковой подсистеме. Введите команду lscfg для каждого порта.
   - В небольших и средних системах введите следующие команды:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - В крупных системах введите следующие команды:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Убедитесь, что установлены следующие наборы файлов AIX:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Введите команду cfgmgr, чтобы система AIX пересканировала оборудование и обнаружила доступные диски. Например:

   ```
   cfgmgr
   ```

4. Чтобы вызвать список доступных дисков, введите следующую команду:

   ```
   lsdev -Ccdisk
   ```

   Должна появиться выходная информация следующего вида:

   ```
   hdisk0  Доступно 00-00-00 SAS Дисковый накопитель
   hdisk1  Доступно 00-00-00 SAS Дисковый накопитель
   hdisk2  Доступно 01-00-00 SAS Дисковый накопитель
   hdisk3  Доступно 01-00-00 SAS Дисковый накопитель
   hdisk4  Доступно 06-01-02 MPIO IBM 2076 Диск ФС
   hdisk5  Доступно 07-01-02 MPIO IBM 2076 Диск ФС
   ...
   ```

5. Используйте выходную информацию команды lsdev, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

   Например, ID устройства может быть `hdisk4`. Сохраните список ID устройств для использования при создании файловых систем для сервера IBM Spectrum Protect.

6. Скоррелируйте ID устройств SCSI с LUN отдельных дисков из дисковой системы, перечислив подробную информацию о всех физических томах в системе. Введите следующую команду:

   ```
   lspv -u
   ```

   В системе IBM® Storwize примером того, что показано для каждого устройства, является следующая информация:

   ```
   hdisk4  00f8cf083fd97327  Нет активен
    332136005076300810105780000000000003004214503IBMfcp
   ```

   В примере значение *600507630081010578000000000000030* - это UID тома, сообщенный интерфейсом управления Storwize.
   Чтобы проверить размер дисков (в мегабайтах) и сравнить его с тем, что указано для системы, введите следующую команду:

   ```
   bootinfo -s hdisk4
   ```

Системы Linux

Процедура

1. Внесите изменения в файл /etc/multipath.conf, чтобы включить поддержку нескольких путей для хостов Linux. Если файл multipath.conf не существует, его можно создать, введя следующую команду:

   ```
   mpathconf --enable
   ```

В файле multipath.conf при тестировании в системе IBM Storwize были заданы следующие параметры:

```
defaults {
             user_friendly_names no
}

devices {
             device {
                          vendor "IBM "
                          product "2145"
                          path_grouping_policy group_by_prio
                          user_friendly_names no
                          path_selector "round-robin 0"
                          prio "alua"
                          path_checker "tur"
                          failback "immediate"
                          no_path_retry 5
                          rr_weight uniform
                          rr_min_io_rq "1"
                          dev_loss_tmo 120
            }
}
```

2. Задайте запуск поддержки нескольких путей при запуске системы. Введите следующие команды:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Чтобы убедиться, что диски видны операционной системе и управляются поддержкой нескольких путей, введите следующую команду:

```
multipath -l
```

4. Убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и ID устройств.
Например, в следующей выходной информации показано, что у диска на 2 ТБ есть две группы путей и четыре активных пути. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула. Используйте часть полного числового ID устройства (в данном примере, 12), чтобы найти том в интерфейсе управления дисковой системой.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
| `- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

   a. Если потребуется, исправьте назначения хостов для LUN диска и произведите принудительное пересканирование шины. Например:

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      Также можно перезапустить систему, чтобы пересканировать назначения хостов для LUN дисков.
   b. Убедитесь, что теперь диски доступны для ввода-вывода по нескольким путям, снова введя команду multipath -l.
5. Используйте выходную информацию команды multipath, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

   Например, ID устройства для вашего диска в 2 ТБ - это `36005076802810c509800000000000012`.

   Сохраните список ID устройств для использования в следующем шаге.

Системы Windows

Процедура

1. Убедитесь, что установлена функция ввода-вывода по нескольким путям. Если потребуется, установите дополнительные драйверы нескольких путей, связанные с поставщиками.
2. Чтобы убедиться, что диски видны операционной системе и управляются вводом-выводом по нескольким путям, введите следующую команду:

   ```
   c:\program files\IBM\SDDDSM\datapath.exe query device
   ```

3. Ознакомьтесь с выходной информацией для поддержки нескольких путей и убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и серийных номерах устройств.
   Например, используя часть полного серийного номера устройства (в данном примере, 34), вы сможете искать том в интерфейсе управления дисковой системой. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула хранения.

   ```
   № УСТР.   4  ИМЯ УСТРОЙСТВА: Disk5 Part0   ТИП: 2145    ПОЛИТИКА: ОПТИМИЗИРОВАННАЯ
   СЕР.НОМ.: 600507630081010578000000000000034          РАЗМЕР LUN: 2.0 ТБ
   ============================================================================
   № пути       Адаптер/Жесткий диск    Состояние  Режим      Выбор    Ошибки
       0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0        0
       1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176        0
       2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494        0
       3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0        0
   ```

4. Создайте список ID дисковых устройств, используя серийные номера, возвращенные в выходной информации нескольких путей в предыдущем шаге.

   Например, ID устройства для вашего диска в 2 ТБ - это `600507630081010578000000000000034`

   Сохраните список ID устройств для использования в следующем шаге.

5. Чтобы привести новые диски в подключенное состояние и снять атрибут "только для чтения", выполните diskpart.exe со следующими командами. Повторите для каждого из дисков:

   ```
   diskpart
      select Disk 1
      online disk
      attribute disk clear readonly
      select Disk 2
      online disk
      attribute disk clear readonly
      < ... >
      select Disk 49
      online disk
      attribute disk clear readonly
      exit
   ```

Создание ID пользователя для сервера

Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.

Об этой задаче

В ID пользователя можно использовать только буквы в нижнем регистре (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:

- Длина не должна превышать 8 символов.
- ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
- В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

Процедура

1. Чтобы создать ID пользователя, используйте команды операционной системы.
   -  Операционные системы AIX  Операционные системы LinuxСоздайте группу и ID пользователя в домашнем каталоге пользователя, который станет владельцем экземпляра сервера.

Например, чтобы создать ID пользователя tsminst1 в группе tsmsrvrs с паролем tsminst1, введите от имени ID административного пользователя следующие команды:

 Операционные системы AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

 Операционные системы Linux

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Выйдите из системы, затем снова в нее войдите. Перейдите на созданную вами учетную запись пользователя. Используйте интерактивную программу входа в систему, например, telnet, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.

-  Операционные системы WindowsСоздайте ID пользователя, а затем добавьте новый ID в группу администраторов. Например, чтобы создать ID пользователя tsminst1, введите следующую команду:

```
net user tsminst1 * /add
```

После создания и проверки пароля для нового пользователя добавьте ID пользователя в группу Администраторы, введя следующие команды:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Завершите сеанс для нового ID пользователя.

Подготовка файловых систем для сервера

Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

- Подготовка файловых систем в системах AIX
  Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.
- Подготовка файловых систем в системах Linux
  Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.
- Подготовка файловых систем в системах Windows
  Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Подготовка файловых систем в системах AIX

Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.

Процедура

1. Увеличьте глубину очереди и максимальный размер передачи для всех доступных дисков *hdiskX*. Введите для каждого диска следующие команды:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

   Не выполняйте эти команды для внутренних дисков операционной системы, например, для *hdisk0*.
2. Создайте группы томов для базы данных, активного журнала, архивного журнала, резервного копирования базы данных и пула хранения IBM Spectrum Protect. Введите команду mkvg, указав ID устройств для соответствующих дисков, которые вы указали ранее.

Например, если имена устройств *hdisk4, hdisk5* и *hdisk6* соответствуют дискам базы данных, включите их в группу томов базы данных и т.д.
Размер системы: Приведенные ниже команды основаны на конфигурации системы среднего размера. Для малых и больших систем необходимо соответствующим образом настроить синтаксис.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Определите имена физического тома и число свободных физических разделов, которые следует использовать при создании логических томов. Введите команду lsvg для каждой группы томов, которую вы создали в предыдущем шаге.
   Например:

   ```
   lsvg -p tsmdb
   ```

   Вывод будет подобен следующему. В столбце *FREE PPs* представлены свободные физические разделы:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Создайте логические тома в каждой группе томов при помощи команды mklv. Размер томов, группа томов и имена устройств будут разными в зависимости от размера вашей системы и различий в конфигурации дисков.
   Например, чтобы создать тома для базы данных IBM Spectrum Protect в системе среднего размера, введите следующие команды:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Сформатируйте файловые системы на каждом логическом томе, используя команду crfs.
   Например, чтобы сформатировать файловые системы для базы данных в системе среднего размера, введите следующие команды:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Смонтируйте все заново созданные файловые системы, введя следующую команду:

   ```
   mount -a
   ```

7. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере выходной информации команды показано, что объем используемого пространства, как правило, составляет 1%:

   ```
   tapsrv07> df -g /tsminst1/*
   Файловая сист. Блоки ГБ   Свободно  % исп. Мое исп. % моего исп. Смонтировано
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Убедитесь, что у ID пользователя, созданного вами в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам на сервере IBM Spectrum Protect.

Подготовка файловых систем в системах Linux

Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.

Процедура

1. Используя список ID устройств, сгенерированный ранее, введите команду mkfs, чтобы создать и сформатировать файловую систему для каждого устройства LUN хранения. Укажите ID устройства в команде. Смотрите следующую таблицу. Для базы данных сформатируйте файловые системы ext4:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Для LUN пула хранения сформатируйте файловые системы xfs:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Команду mkfs можно вводить до 50 раз в зависимости от того, сколько разных устройств у вас есть.

2. Создайте каталоги точек монтирования для файловых систем.

   Введите команду mkdir для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования.

   Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

   ```
   mkdir /tsminst1
   ```

   Повторите команду mkdir для каждой файловой системы.
3. Добавьте в файл /etc/fstab запись для каждой файловой системы, чтобы файловые системы монтировались автоматически при запуске сервера.
   Например:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Смонтируйте файловые системы, которые вы добавили в файл /etc/fstab, введя команду mount -a.
5. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере в системе IBM® Storwize показано, что объем используемого пространства, как правило, составляет 1%:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Файловая сист.                                  Размер Исп. Дост. Исп. % Где смонтир.
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```

6. Убедитесь, что у ID пользователя, созданного вами в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам для IBM Spectrum Protect.

Подготовка файловых систем в системах Windows

Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Процедура

1. Создайте каталоги точек монтирования для файловых систем.
   Введите команду md для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования. Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

   ```
   md c:\tsminst1
   ```

   Повторите команду md для каждой файловой системы.
2. Создайте том для каждого LUN диска, отображенного в каталог в каталоге экземпляра сервера с использованием менеджера томов Windows.

   Выберите Менеджер серверов > Службы файлов и хранения и выполните описанные ниже шаги для каждого диска, соответствующего отображению LUN, созданному в предыдущем шаге:

   a. Переведите диск в подключенное состояние.
   b. Инициализируйте диск до базового типа GPT, который является типом по умолчанию.
   c. Создайте простой том, занимающий все пространство на диске. Сформатируйте файловую систему с использованием NTFS и задайте метку, соответствующую назначению тома, например, TSMfile00. Не

назначайте для нового тома букву диска. Вместо этого отобразите том в каталог в каталоге экземпляра, например, в C:\tsminst1\TSMfile00.
Совет: Определите метку тома и метки отображений каталога на основе сообщенного размера диска.

3. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Вызовите список всех файловых систем, введя команду mountvol и ознакомившись с выходной информацией. Например:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
  C:\tsminst1\TSMdbspace00\
```

4. По завершении конфигурирования диска перезапустите систему.

Дальнейшие действия

Вы можете подтвердить объем свободного пространства для каждого тома, используя Проводник Windows.

Установка сервера и компонента Центр операций

Используйте для установки компонентов графический мастер IBM® Installation Manager.

- Установка в системах AIX и Linux
  Установите сервер IBM Spectrum Protect и Центр операций в первой серверной системе.
- Установка в системах Windows
  Установите сервер IBM Spectrum Protect и Центр операций в первой серверной системе.

Установка в системах AIX и Linux

Установите сервер IBM Spectrum Protect и Центр операций в первой серверной системе.

Прежде чем начать

Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

1. Операционные системы AIXУбедитесь, что у вас в системе установлены необходимые файлы RPM.

   Дополнительные сведения смотрите в разделе Установка обязательных файлов RPM для графического мастера.

2. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042992.
3. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
4. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

   ```
   chmod a+x имя_пакета.bin
   ```

5. Извлеките пакет, введя следующую команду:

   ```
   ./имя_пакета.bin
   ```

   где *имя_пакета* - это имя скачанного файла.
6. Операционные системы AIXУбедитесь, что включена следующая команда, чтобы мастера работали правильно:

   ```
   lsuser
   ```

   По умолчанию эта команда включена.
7. Перейдите в каталог, куда вы поместили исполняемый файл.
8. Запустите мастер установки, введя следующую команду:

   ```
   ./install.sh
   ```

Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

- Установка обязательных файлов RPM для графического мастера
  Файлы RPM необходимы для графического мастера IBM Installation Manager.

Задачи, связанные с данной:
Другие методы установки компонентов IBM Spectrum Protect (AIX)
Другие методы установки компонентов IBM Spectrum Protect (Linux)

Установка в системах Windows

Установите сервер IBM Spectrum Protect и Центр операций в первой серверной системе.

Прежде чем начать

Убедитесь, что выполнены следующие обязательные требования:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
- Убедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

1. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042993.
2. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
3. Перейдите в каталог, куда вы поместили исполняемый файл.
4. Дважды щелкните по выполняемому файлу, чтобы извлечь его в текущий каталог.
5. В каталоге, куда были распакованы файлы установки, запустите мастер установки, дважды щелкнув по файлу install.bat. Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager.

  Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Задачи, связанные с данной:
Другие методы установки компонентов IBM Spectrum Protect

Конфигурирование сервера и компонента Центр операций

После установки компонентов выполните конфигурирование сервера IBM Spectrum Protect и компонента Центр операций.

- Конфигурирование экземпляра сервера
  Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.
- Установка клиента резервного копирования и архивирования
  Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.
- Как задать опции для сервера
  Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.
- Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)
  Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.
- Конфигурирование Центра операций
  После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.
- Регистрация лицензии на продукт
  Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.
- Конфигурирование дедупликации данных
  Создайте пул хранения каталогов-контейнеров и хотя бы один каталог пула хранения, чтобы использовать встроенную дедупликацию данных.
- Как задать правила хранения данных для вашего бизнеса
  После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.
- Как задать расписания для операций по обслуживанию сервера
  Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.
- Определение расписаний клиентов
  Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Конфигурирование экземпляра сервера

Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.

Прежде чем начать

Убедитесь, что выполнены следующие требования:
Операционные системы AIX Операционные системы Linux

- В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
- В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле sshd_config в каталоге /etc/ssh/. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения *localhost*.
- Вы должны иметь возможность войти в IBM Spectrum Protect, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
- Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Операционные системы WindowsУбедитесь, что служба удаленного реестра запущена, выполнив следующие шаги:

1. Выберите Пуск > Администрирование > Службы. В окне Службы выберите Удаленный реестр. Если служба не запущена, щелкните по Пуск.
2. Убедитесь, что порты 137, 139 и 445 не заблокированы брандмауэром:
    a. Щелкните по Запуск > Панель управления > Брандмауэр Windows.
    b. Выберите Дополнительные параметры.
    c. Выберите Входные правила.
    d. Выберите Новое правило.
    e. Создайте правило порта для портов TCP 137, 139 и 445, чтобы разрешить соединения для доменных и частных сетей.
3. Сконфигурируйте управление учетными записями пользователей, получив доступ к опциям Локальная политика безопасности и выполнив следующие шаги:
    a. Щелкните по Пуск > Администрирование > Локальная политика безопасности. Разверните Локальные политики > Опции безопасности.
    b. Если эта возможность еще не включена, включите встроенную учетную запись администратора, выбрав Учетные записи: Состояние учетной записи администратора > Включить > ОК.
    c. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для всех администраторов Windows, выбрав Управление учетными записями пользователей: Запускать всех администраторов в режиме утверждения администраторов > Выключить > ОК.
    d. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для встроенной учетной записи администратора, выбрав Управление учетными записями пользователей: Режим утверждения администраторов для встроенной учетной записи администратора > Выключить > ОК.
4. Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Об этой задаче

Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

Процедура

1. Запустите локальную версию мастера.
    - Операционные системы AIXОперационные системы LinuxОткройте программу dsmicfgx в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запустить только от имени пользователя root.
    - Операционные системы WindowsЩелкните по Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования.
2. Завершите конфигурирование, следуя инструкциям. Используйте информацию, записанную вами в таблицу Рабочие листы планирования в ходе настройки системы IBM Spectrum Protect, чтобы задать каталоги и опции в мастере.

    Операционные системы AIXОперационные системы LinuxВ окне Информация о сервере задайте автоматический запуск сервера при загрузке системы, используя ID пользователя экземпляра.

    Операционные системы WindowsПри использовании мастера конфигурирования для сервера будет задан автоматический запуск при перезагрузке.

Установка клиента резервного копирования и архивирования

Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.

Процедура

Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.

- Установить клиентов резервного копирования и архивирования UNIX и Linux
- Первая установка клиента Windows

Как задать опции для сервера

Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.

Процедура

1. Перейдите в каталог экземпляра сервера и откройте файл dsmserv.opt.
2. Ознакомьтесь со следующими значениями в таблице и проверьте параметры опций сервера на основе размера системы.

Серверный параметр	Значение для небольшой системы	Значение для средней системы	Значение для крупной системы
ACTIVELOGDIRECTORY	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Да	Нет	Нет
ARCHLOGDIRECTORY	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации	Путь каталога, заданный во время конфигурации
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	Нет	Нет	Нет
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Обновите параметры опций сервера, если потребуется, чтобы они соответствовали значениям в таблице. Чтобы внести обновления, закройте файл dsmserv.opt и воспользуйтесь командой SETOPT в интерфейсе командной строки администрирования, чтобы задать опции.
Например, чтобы обновить опцию IDLETIMEOUT до 60, введите следующую команду:

```
setopt idletimeout 60
```

3. Чтобы сконфигурировать защищенную связь с сервером, клиентами и Центр операций, то проверьте опции в следующей таблице:

Серверный параметр	Системы всех размеров
SSLFIPSMODE	NO
TCPPORT	Задайте номер порта, на котором сервер ожидает требований установления сеансов TCP/IP и SSL от клиента.
TCPADMINPORT	Задайте адрес порта, на котором сервер ожидает требований установления сеансов TCP/IP и SSL от клиента администрирования с интерфейсом командной строки.

Если нужно обновить любое из значений опций, измените файл dsmserv.opt, используя следующие рекомендации:
   - Чтобы включить опцию, удалите звездочку в начале строки.
   - В каждой строке введите только одну опцию и заданное для нее значение.
   - Если опция встречается в нескольких записях в файле, сервер будет использовать последнюю запись.

Сохраните свои изменения файл и закройте файл. Если вы непосредственно внесете изменения в файл dsmserv.opt, вы должны будете перезапустить сервер, чтобы изменения вступили в силу.

Ссылки, связанные с данной:
Справочник по опциям сервера
SETOPT (Задать динамическое обновление серверной опции)

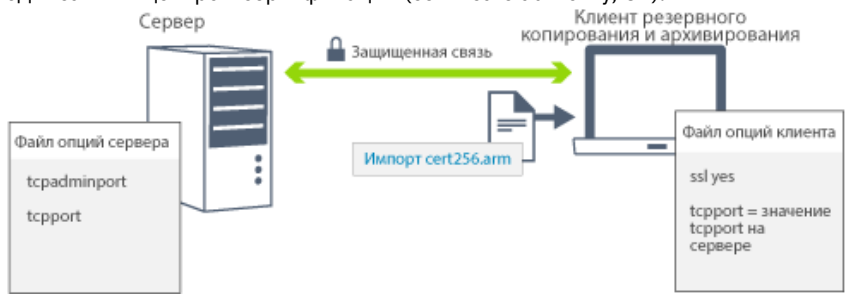
Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)

Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.

Об этой задаче

Начиная с версии 8.1.2 IBM Spectrum Protect, SSL включен по умолчанию, а сервер IBM Spectrum Protect и клиент резервного копирования и архивации автоматически конфигурируются для обмена данными с помощью протокола TLS 1.2.

Как показано на следующем рисунке, вы можете вручную сконфигурировать защищанную связь между сервером и клиентом резервного копирования и архивирования, задав опции в файлах опций сервера и клиента, а затем перенеся на клиент самоподписанный сертификат, сгенерированный на сервере. Либо можно получить уникальный сертификат, подписанный центром сертификации (certificate authority, CA).



Дополнительную информацию о конфигурировании сервера и клиентов для взаимодействий SSL или TLS смотрите в разделе Конфигурирование агентов хранения, серверов, клиентов и центра операций для соединения с сервером с использованием SSL.

Конфигурирование Центра операций

После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.

Прежде чем начать

Если вы подключаетесь к компоненту Центр операций впервые, вы должны предоставить следующую информацию:

- Информация о соединении для сервера, который вы хотите назначить хаб-сервером
- Идентификационные данные входа в систему для администратора, который задан для этого сервера

Процедура

1. Определите хаб-сервер. Введите в окне веб-браузера следующий адрес:

   `https://`*`имя_хоста`*`:`*`защищенный_порт`*`/oc`

   Здесь используются следующие обозначения:
   - *имя_хоста* - это имя компьютера, где установлен компонент Центр операций
   - *защищенный_порт* - это номер порта, используемого компонентом Центр операций для HTTPS-взаимодействий на этом компьютере

   Например, если имя хоста - это tsm.storage.mylocation.com и вы используете для компонента Центр операций защищенный порт по умолчанию, адрес пример следующий вид:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

Когда вы впервые входите в компонент Центр операций, мастер поможет вам выполнить первоначальное конфигурирование, чтобы задать нового администратора с системными полномочиями на сервере.

2. Настройте защищенные взаимодействия между компонентом Центр операций и хаб-сервером, сконфигурировав протокол Secure Sockets Layer (SSL).

   Следуйте инструкциям в разделе Защита связи между компонентом Центр операций и хаб-сервером.

3. Необязательно: Чтобы ежедневно получать по электронной почте отчет, в котором суммируется состояние системы, сконфигурируйте параметры электронной почты в компоненте Центр операций.

   Следуйте инструкциям в разделе Состояние системы отслеживания с использованием отчетов по электронной почте.

- Защита связи между компонентом Центр операций и хаб-сервером
  Для защиты связи между компонентом Центр операций и хаб-сервером добавьте сертификат Transport Layer Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Регистрация лицензии на продукт

Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.

Об этой задаче

Лицензии хранятся в файлах сертификата регистрации, который содержит сведения о лицензировании для продукта. Файлы регистрационных сертификатов находятся на носителе установки и при установке помещаются на сервер. После регистрации продукта лицензии хранятся в NODELOCK-файле в текущем каталоге.

Процедура

Зарегистрируйте лицензию, указав имя файла сертификата регистрации, содержащего лицензию. Чтобы использовать построитель команд Центр операций для этой задачи, выполните следующие шаги:

1. Откройте Центр операций.
2. Откройте построитель команд компонента Центр операций, установив указатель мыши на значок параметров  и щелкнув по Построитель команд.
3. Введите команду REGISTER LICENSE. Например, чтобы зарегистрировать базовую лицензию IBM Spectrum Protect, введите следующую команду:

   ```
   register license file=tsmbasic.lic
   ```

Дальнейшие действия

Сохраните носитель установки, на котором содержатся файлы сертификата регистрации. Возможно, вам придется снова зарегистрировать лицензию, если, например, возникнет одно из следующих условий:

- Сервер перенесен на другой компьютер;
- Файл NODELOCK поврежден. Сервер сохраняет данные лицензий в файле NODELOCK, расположенном в каталоге, из которого запускается сервер.
- Операционные системы LinuxВы изменяете микросхему процессора, связанную с сервером, на котором установлен сервер.

Ссылки, связанные с данной:
REGISTER LICENSE (регистрация новой лицензии)

Конфигурирование дедупликации данных

Создайте пул хранения каталогов-контейнеров и хотя бы один каталог пула хранения, чтобы использовать встроенную дедупликацию данных.

Прежде чем начать

Используйте при выполнении этой задачи информацию о каталоге пула хранения данных, которую вы записали в разделе Рабочие листы планирования.

Процедура

1. Откройте Центр операций.
2. В строке меню Центр операций установите указатель мыши на Хранилище.
3. В появившемся списке щелкните по Пулы хранилищ.
4. Щелкните по кнопке + Пул хранилищ.
5. Выполните шаги в мастере Добавить пул хранения:
   - Чтобы использовать встроенную дедупликацию данных, выберите пул хранения Каталог в хранилище на основе контейнеров.
   - При конфигурировании каталогов для пула хранения каталогов-контейнеров задайте пути каталогов, которые вы создали для хранения во время настройки системы.
6. После того как вы сконфигурируете новый пул хранения каталогов-контейнеров, щелкните по Закрыть и просмотреть политики, чтобы обновить класс управления и начать использовать пул хранения.

Как задать правила хранения данных для вашего бизнеса

После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.

Процедура

1. На странице Службы в Центр операций выберите домен STANDARD и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики. На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.
3. Щелкните по переключателю Конфигурировать и внесите следующие изменения:
   - Измените объект назначения резервного копирования для класса управления STANDARD, задав пул хранения каталога-контейнера.
   - Измените значение в столбце Резервные копии на Без ограничения.
   - Измените срок хранения. Задайте в столбце Хранить лишние резервные копии значение 30 дней или более в зависимости от ваших бизнес-требований.
4. Сохраните изменения и щелкните по переключателю Конфигурировать, чтобы набор политик стал недоступен для изменения.
5. Активируйте набор политик, для чего щелкните по Активировать.

Задачи, связанные с данной:
Как задать роли для резервного копирования и архивирования данных клиента

Как задать расписания для операций по обслуживанию сервера

Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.

Об этой задаче

Запланируйте операции обслуживания сервера, так чтобы они выполнялись после операций резервного копирования клиента. Вы можете управлять синхронизацией расписаний, задав время начала в сочетании с длительностью каждой операции.

В приведенном ниже примере показано, как можно запланировать процессы обслуживания сервера в сочетании с расписанием резервного копирования клиента для дискового решения с несколькими площадками.

Операция	**Запланированное задание**
Резервное копирование клиента	Начинается в 22:00.
Репликация узлов	Начинается в 08:00 или через 10 часов после начала резервного копирования клиента.

Операция	Запланированное задание
Обработка базы данных и файлов аварийного восстановления	• Резервное копирование базы данных начинается в 11:00 или через 13 часов после начала резервного копирования клиента. Этот процесс выполняется до его завершения. • Информация о конфигурации устройства и резервное копирование хронологии томов запускаются в 17:00 или спустя 6 часов после запуска резервного копирования базы данных. • Удаление хронологии томов запускается в 20:00 или спустя 9 часов после запуска резервного копирования базы данных.
Устаревание инвентарного перечня	Начинается в 12:00 или через 14 часов после начала окна резервного копирования клиента. Этот процесс выполняется до его завершения.

Процедура

После того как вы сконфигурируете класс устройств для резервных копий базы данных, создайте расписания для резервного копирования базы данных и других необходимых операций обслуживания, используя команду DEFINE SCHEDULE. В зависимости от размера вашей среды вам, возможно, придется скорректировать время запуска для каждого расписания в примере.

1. Определить класс устройства для операций резервного копирования. Например, используйте команду DEFINE DEVCLASS, чтобы создать класс устройств с именем DBBACK_FILEDEV:

   ```
   define devclass dbback_filedev devtype=file
     directory=каталоги_резервных_копий_бд
   ```

   где *каталоги_резервных_копий_бд* - это список каталогов, которые вы создали для резервных копий базы данных. Операционные системы AIX Операционные системы LinuxНапример, если у вас есть четыре каталога для резервных копий базы данных, начиная с /tsminst1/TSMbkup00, введите следующую команду:

   ```
   define devclass dbback_filedev devtype=file
     directory=/tsminst1/TSMbkup00,
     /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
     /tsminst1/TSMbkup03"
   ```

   Операционные системы WindowsНапример, если у вас есть четыре каталога для резервных копий базы данных, начиная с C:\tsminst1\TSMbkup00, введите следующую команду:

   ```
   define devclass dbback_filedev devtype=file
     directory="c:\tsminst1\TSMbkup00,
     c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
   ```

2. Задайте класс устройств для операций автоматического резервного копирования базы данных. Используйте команду SET DBRECOVERY, чтобы указать класс устройств, созданный вами в предыдущем шаге. Например, если класс устройств - это dbback_filedev, введите следующую команду:

   ```
   set dbrecovery dbback_filedev
   ```

3. Создайте расписания для операций обслуживания, используя команду DEFINE SCHEDULE. Обязательные операции с примерами команд смотриет в следующей таблице.
   Совет: В последующем шаге вы создадите отдельное расписание для репликации, когда будете использовать компонент Центр операций для конфигурирования репликации.

Операция	Пример команды

Операция	Пример команды
Создайте резервную копию базы данных.	Создайте расписание, чтобы выполнить команду BACKUP DB. Если вы конфигурируете небольшую систему, задайте для параметра COMPRESS значение YES. Например, в небольшой системе введите следующую команду, чтобы создать расписание резервного копирования, использующее новый класс устройств: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Создать рез. копию базы данных." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Создайте резервную копию информации о конфигурации устройств.	Создайте расписание, чтобы выполнить команду BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Создать рез. копию файла конфигурации устройства." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Создайте резервную копию хронологии томов.	Создайте расписание, чтобы выполнить команду BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Создать резервную копию хронологии томов." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Удалите более старые версии резервных копий базы данных, которые больше не требуются.	Создайте расписание, чтобы выполнить команду DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Удалить старые резервные копии базы данных." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Удалите объекты, у которых превышен допустимый срок хранения.	Создайте расписание, чтобы выполнить команду EXPIRE INVENTORY. Задайте параметр RESOURCE на основе размера системы, которую вы конфигурируете: ○ Небольшие системы: 10 ○ Средние системы: 30 ○ Крупные системы: 40 Например, в системе среднего размера, введите следующую команду, чтобы создать расписание с именем EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Удалить проср. объекты." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Дальнейшие действия

После того как вы создадите расписания задач по обслуживанию сервера, вы сможете увидеть их в компоненте Центр операций, выполнив следующие шаги:

1. В строке меню Центр операций установите указатель мыши на Серверы.
2. Щелкните по Обслуживание.

Ссылки, связанные с данной:
DEFINE SCHEDULE (определение расписания выполнения административных команд)

Определение расписаний клиентов

Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Процедура

1. В строке меню Центр операций установите указатель мыши на Клиенты.
2. Щелкните по Расписания.
3. Щелкните по + Расписание.
4. Выполните шаги в мастере Создать расписание. Задайте запуск расписаний резервного копирования клиента в 22:00, основываясь на операциях по обслуживанию сервера, которые вы запланировали в разделе Как задать расписания для операций по обслуживанию сервера.

Установка и конфигурирование клиентов резервного копирования и архивирования

После успешной настройки системы сервера IBM Spectrum Protect установите и сконфигурируйте программу клиента, чтобы начать резервное копирование данных.

Процедура

Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.

- Установить клиентов резервного копирования и архивирования UNIX и Linux
- Первая установка клиента Windows

Дальнейшие действия

Зарегистрируйте свои клиенты и назначьте их для расписаний.

- Регистрация и назначение клиентов в расписания
  Добавьте и зарегистрируйте клиенты при помощи компонента Центр операций, воспользовавшись мастером Добавить клиент.
- Установка службы управления клиентом
  Установите службу управления клиентом для клиентов резервного копирования и архивирования, работающих в операционных системах Linux и Windows. Служба управления клиентом собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает эту информацию доступной для компонента Центр операций для базовой возможности мониторинга.

Регистрация и назначение клиентов в расписания

Добавьте и зарегистрируйте клиенты при помощи компонента Центр операций, воспользовавшись мастером Добавить клиент.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию technote 7048963.

Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе Аутентификация пользователей с использованием базы данных Active Directory.

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды REGISTER NODE и задайте параметр USERID:

  ```
  register node имя_узла пароль userid=имя_узла
  ```

  где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе Регистрация узла.
- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центр операций. Сделайте следующее:
  a. В панели меню Центра операций выберите Клиенты.
  b. В таблице Клиенты щелкните по + Клиент.
  c. Выполните шаги в мастере Добавить клиент:
     i. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель Включить в области Дедупликация данных на стороне клиента.
     ii. В окне Конфигурация скопируйте значения TCPSERVERADDRESS, TCPPORT, NODENAME, и DEDUPLICATION.
     Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
     iii. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     iv. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     v. Щелкните по Добавить клиент.

Установка службы управления клиентом

Установите службу управления клиентом для клиентов резервного копирования и архивирования, работающих в операционных системах Linux и Windows. Служба управления клиентом собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает эту информацию доступной для компонента Центр операций для базовой возможности мониторинга.

Процедура

Установите службу управления клиентом на том же компьютере, на котором находится клиент резервного копирования и архивирования, выполнив следующие шаги:

1. Скачайте пакет установки службы управления клиентом с сайта скачиваемых материалов IBM®, например, с сайта IBM Passport Advantage® или IBM Fix Central. Ищите имя файла, аналогичное следующему: `<версия>-IBM_Spectrum_Protect-CMS-операционная_система.bin`.
2. Создайте каталог на компьютере клиента, которым вы хотите управлять, и скопируйте в него пакет установки.
3. Распакуйте контент файла пакета установки.
4. Запустите пакетный файл установки из каталога, в который вы распаковали файлы установки и связанные файлы. Это каталог, который вы создали на шаге 2.
5. Чтобы установить службу управления клиентом, выполните инструкции в мастере IBM Installation Manager. Если на компьютере клиента еще не установлен компонент IBM Installation Manager, вы должны выбрать и IBM Installation Manager, и службу управления клиентом IBM Spectrum Protect.

- Проверка того, правильно ли установлена служба управления клиентами
  Прежде чем использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, вы можете убедиться, что служба управления клиентом правильно установлена и сконфигурирована.
- Конфигурирование Центр операций на использование службы управления клиентом
  Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Задачи, связанные с данной:
Конфигурирование службы управления клиентами для пользовательских установок клиентов

Проверка того, правильно ли установлена служба управления клиентами

Прежде чем использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, вы можете убедиться, что служба управления клиентом правильно установлена и сконфигурирована.

Процедура

Введите на компьютере клиента в командной строке следующие команды, чтобы посмотреть конфигурацию службы управления клиентом:

- На компьютерах клиента Linux введите следующую команду:

  ```
  каталог_установки_клиента/cms/bin/CmsConfig.sh
  list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- На компьютерах клиента Windows введите следующую команду:

  ```
  каталог_установки_клиента\cms\bin\CmsConfig.bat list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Если служба управления клиентами правильно установлена и сконфигурирована, то в выходных результатах показан каталог файла журнала ошибок.
Выходной текст извлекается из следующего файла конфигурации:

- На компьютерах клиента Linux:

  ```
  каталог_установки_клиента/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- На компьютерах клиента Windows:

  каталог_установки_клиента\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Если в выходных результатах нет ни одной записи, то нужно сконфигурировать файл client-configuration.xml. Инструкции по конфигурированию этого файла смотрите в разделе Конфигурирование службы управления клиентами для пользовательских установок клиентов. Можно использовать команду CmsConfig verify, чтобы проверить, правильно ли создано определение узла в файле client-configuration.xml.

Конфигурирование Центр операций на использование службы управления клиентом

Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Прежде чем начать

Убедитесь, что служба управления клиентом установлена и запущена на компьютере клиента. Проверьте, используется ли конфигурация по умолчанию. Конфигурация по умолчанию не используется в следующих случаях:

- Служба управления клиентом не использует номер порта по умолчанию (9028).
- Для клиента резервного копирования и архивирования не используется IP-адрес, который используется для компьютера клиента резервного копирования и архивирования. Например, другой IP-адрес может использоваться в следующих случаях:
  - В компьютерной системе установлено две сетевые карты. Клиент резервного копирования и архивирования сконфигурирован для взаимодействия с одной сетью, а служба управления клиентом взаимодействует с другой сетью.
  - На компьютере клиента используется DHCP. Поэтому компьютеру клиента динамически назначается IP-адрес, сохраненный на сервере во время предыдущей операции клиента резервного копирования и архивирования. При перезагрузке компьютера клиента ему может быть назначен другой IP-адрес. Чтобы Центр операций всегда мог найти компьютер клиента, нужно задать полное имя домена.

Процедура

Чтобы сконфигурировать Центр операций для использования службы управления клиентом, сделайте следующее:

1. Выберите клиента на странице Клиенты Центра операций.
2. Выберите Сведения > Свойства.
3. В поле URL удаленной диагностики в разделе Общие задайте URL для службы управления клиентом в системе клиента. Адрес должен начинаться с `https`. В следующей таблице показаны примеры URL удаленной диагностики.

Тип URL	**Пример**
С именем хоста DNS и портом по умолчанию (9028)	https://server.example.com
С именем хоста DNS и портом не по умолчанию	https://server.example.com:1599
С IP-адресом и портом не по умолчанию	https://192.0.2.0:1599

4. Щелкните по Сохранить.

Дальнейшие действия

Вы можете получить доступ к диагностической информации о клиенте (например, к файлам журнала клиента) на вкладке Диагностика в Центре операций.

Конфигурирование второго сервера

После завершения конфигурирования первого сервера в вашей системе сконфигурируйте второй сервер.

Процедура

Следуйте инструкциям в следующих разделах:

1. Сконфигурируйте второй сервер, который является таким же, как и первый сервер, выполнив инструкции в следующих разделах:
    a. Настройка системы
    b. Установка сервера и компонента Центр операций

       В дисковом решении с несколькими площадками в качестве хаб-сервера конфигурируется только один сервер, поэтому вам не нужно устанавливать компонент Центр операций на втором сервере. Выбирая пакеты установки для установки на втором сервере, не выбирайте Центр операций.

    c. Конфигурирование сервера и компонента Центр операций

       Пропустите задачи по конфигурированию компонента Центр операций.

    d. Установка и конфигурирование клиентов резервного копирования и архивирования
2. Конфигурирование связи SSL между хаб-сервером и подчиненным сервером
3. Добавление второго сервера как подчиненного сервера
4. Как включить репликацию

Конфигурирование связи SSL между хаб-сервером и подчиненным сервером

Чтобы защитить связь между хаб-сервером и подчиненным сервером с использованием протокола Transport Layer Security (TLS), нужно задать на хаб-сервере сертификат подчиненного сервера.

Об этой задаче

Хаб-сервер получает информацию об оповещениях и состоянии от подчиненного сервера и показывает эту информацию в компоненте Центр операций. Чтобы получить информацию о состоянии и оповещениях от подчиненного сервера, сертификат подчиненного сервера нужно добавить в файл доверенных сертификатов хаб-сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.

Чтобы включить другие функции компонента Центр операций, например, автоматическое внедрение обновлений клиента, сертификат хаб-сервера нужно добавить в файл доверенных сертификатов подчиненного сервера.

Процедура

1. Выполните следующие шаги, чтобы задать сертификат подчиненного сервера для хаб-сервера:
    a. На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.
    b. Задайте необходимый сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей подчиненного сервера. Введите следующую команду:

       ```
       gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
        -label "TSM Server SelfSigned SHA Key"
       ```

    c. Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

       ```
       gsk8capicmd_64 -cert -list -db cert.kdb -stashed
       ```

    d. Передайте безопасным способом файл cert256.arm подчиненного сервера на хаб-сервер.
    e. На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
    f. Задайте сертификат подчиненного сервера на хаб-сервере. Введите указанную ниже команду в каталоге экземпляра хаб-сервера, где *имя_подчиненного_сервера* - это имя подчиненного сервера, а *подчиненный_cert256.arm* - имя файла сертификата подчиненного сервера:

       ```
       gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
        -label имя_подчиненного_сервера -file подчиненный_cert256.arm
       ```

2. Выполните следующие шаги, чтобы задать сертификат хаб-сервера для подчиненного сервера:
    a. На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
    b. Задайте необходимый сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера. Введите следующую команду:

       ```
       gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
        -label "TSM Server SelfSigned SHA Key"
       ```

c. Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

d. Передайте безопасным способом файл cert256.arm хаб-сервера на подчиненный сервер.
e. На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.
f. Задайте сертификат хаб-сервера для подчиненного сервера. Введите указанную ниже команду из каталога экземпляра подчиненного сервера, где *имя_хаб_сервера* - это имя хаб-сервера, а *хаб_cert256.arm* - это имя файла сертификата хаб-сервера:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
 -label имя_хаб_сервера -file хаб_cert256.arm
```

3. Перезапустите хаб-сервер и подчиненный сервер.
4. Выполните следующие шаги, чтобы задать подчиненный сервер для хаб-сервера и хаб-сервер для подчиненного сервера:
   a. Введите на хаб-сервере и на подчиненном сервере следующие команды:

```
SET SERVERPASSWORD пароль_сервера
SET SERVERHLADDRESS ip_адрес
SET SERVERLLADDRESS порт_tcp
```

   b. На хаб-сервере введите команду DEFINE SERVER в соответствии со следующим примером:

```
DEFINE SERVER имя_подчиненного_сервера HLA=адрес_подчиненного_сервера
 LLA=spoke_SSLTCPADMINPort SERVERPA=пароль_подчиненного_сервера
```

   c. На подчиненном сервере введите команду DEFINE SERVER в соответствии со следующим примером:

```
DEFINE SERVER имя_хаб_сервера HLA=адрес_хаба
 LLA=hub_SSLTCPADMINPort SERVERPA=пароль_хаб_сервера
```

   Совет: По умолчанию, взаимодействия с сервером шифруются за исключением случаев, когда сервер отправляет или принимает данные объектов. Данные объектов отправляются и принимаются с использованием TCP/IP. Если выбрать опцию, запрещающую шифровать данные объекта, производительность сервера будет аналогична взаимодействиям в сеансе TCP/IP, и сеанс будет защищен. Чтобы зашифровать все взаимодействия с указанным сервером, даже если сервер отправляет или принимает данные объектов, задайте параметр SSL=YES в команде DEFINE SERVER.
5. Выполните следующие шаги, чтобы сконфигурировать Центр операций для мониторинга подчиненного сервера:
   a. В строке меню компонента Центр операций щелкните по Серверы. Подчиненный сервер будет находиться в состоянии "Без мониторинга". Это состояние означает, что, хотя этот сервер задан для хаб-сервера с использованием команды DEFINE SERVER, сервер еще не сконфигурирован как подчиненный сервер.
   b. Щелкните по подчиненному серверу, чтобы выделить элемент, и щелкните по Отслеживать подчиненный.

Ссылки, связанные с данной:
DEFINE SERVER (Задать сервер для обмена данными между серверами)
QUERY OPTION (Запросить информацию о серверных опциях)

Добавление второго сервера как подчиненного сервера

После того как вы сконфигурируете оба сервера в вашей среде, добавьте второй сервер в качестве подчиненного на хаб-сервер.

Процедура

1. Откройте Центр операций.
2. Щелкните в панели меню Центр операций по Серверы.
3. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по Отслеживать подчиненный.
   - Если сервера, который вы хотите добавить, нет в таблице, щелкните по + Подчиненный.
4. Выполните инструкции мастера конфигурирования подчиненных серверов.

Как включить репликацию

Чтобы защитить данные, включите репликацию узла в дополнение к защите ваших пулов хранения.

Процедура

Чтобы включить репликацию узлов для всех клиентов, зарегистрированных на исходном сервере, выполните следующие шаги

1. Откройте Центр операций.
2. В строке меню компонента Центр операций установите указатель мыши на Хранение и щелкните по Репликация.
3. На странице Репликация щелкните по + Пара серверов.
4. Выполните шаги в мастере Добавить пару серверов:
    - Задайте исходный сервер как первый сервер, который вы сконфигурировали для дискового решения с несколькими площадками. Вторым сервером является целевой сервер.
    - Задайте расписание репликации узла, так чтобы оно начиналось через 10 часов после окна резервного копирования клиента в соответствии с операциями по обслуживанию сервера, запланированными вами в разделе Как задать расписания для операций по обслуживанию сервера.
    - Мастер настраивает для вас расписания защиты пула хранения на основе объема защищаемых данных, а также когда планируется репликация клиента.

Дальнейшие действия

Если вы собираетесь настроить взаимную репликацию между двумя площадками, снова запустите мастер Добавить пару серверов и задайте второй сервер как источник, а первый сервер - как назначение.

Завершение реализации

После того, как решение IBM Spectrum Protect будет сконфигурировано и заработает, проверьте операции резервного копирования и настройте мониторинг, чтобы убедиться, что все нормально работает.

Процедура

1. Проверьте операции резервного копирования, чтобы убедиться, что ваши данные защищены, как вы и ожидали.
    a. Выберите на странице Клиенты компонента Центр операций клиенты, для которых вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
    b. На странице Серверы в компоненте Центр операций выберите сервер, для которого вы хотите производить резервное копирование базы данных. Щелкните по Резервное копирование и выполните инструкции в окне Резервное копирование базы данных.
    c. Убедитесь, что резервное копирование выполнено без предупреждений или сообщений об ошибках.
    Совет: Либо можно использовать графический интерфейс клиента резервного копирования и архивирования для резервного копирования данных клиента, и можно производить резервное копирование базы данных, вводя команду BACKUP DB из административной командной строки.
2. Настройте мониторинг для ваших решений, следуя инструкциям в разделе Мониторинг дискового решения с несколькими площадками.

Мониторинг дискового решения с несколькими площадками

После реализации дискового решения IBM Spectrum Protect с несколькими площадками произведите мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.

Об этой задаче

Предпочтительный способ мониторинга решения заключается в использовании компонента Центр операций, который позволяет получить общее и подробное состояние системы в графическом пользовательском интерфейсе. Кроме того, можно сконфигурировать центр операций для генерирования ежедневного отчета по электронной почте, в котором суммируется состояние системы.

В некоторых случаях для выполнения отдельных задач по мониторингу или устранению ошибок вам может потребоваться использовать расширенные инструменты мониторинга.

Совет: Если вы собираетесь диагностировать проблемы клиентов резервного копирования и архивирования в операционных системах Linux или Windows, установите службу управления клиентом IBM Spectrum Protect на каждом компьютере, где установлен клиент резервного копирования и архивирования. Таким образом можно обеспечить нахождение кнопки Диагностика в компоненте Центр операций для диагностики проблем клиентов резервного копирования и архивирования. Чтобы установить службу управления клиентом, выполните инструкции в разделе Установка службы управления клиентом.

Процедура

1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе Контрольный список ежедневного мониторинга.
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе Контрольный список периодического мониторинга.
3. Чтобы проверить, соответствует ли ваше решение IBM Spectrum Protect требованиям по лицензированию, следуйте инструкциям в разделе Проверка на соответствие лицензии.
4. Как сконфигурировать центр операций для генерирования отчетов о состоянии электронной почты, смотрите в разделе Состояние системы отслеживания с использованием отчетов по электронной почте

Дальнейшие действия

Устраните все обнаруженные вами проблемы. Чтобы устранить проблему, изменив конфигурацию вашего решения, следуйте инструкциям в разделе Управление операциями для дискового решения с несколькими площадками. Кроме того, существуют следующие ресурсы:

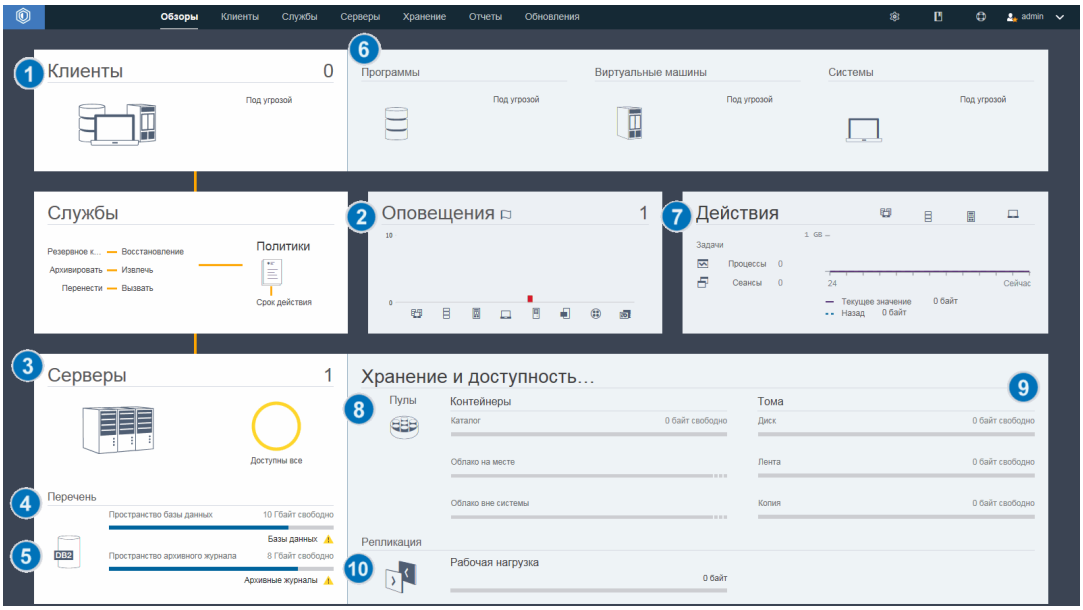
- Информацию об устранении проблем производительности смотрите в разделе Производительность.
- Информацию об устранении других проблем смотрите в разделе Устранение неполадок.

Контрольный список ежедневного мониторинга

Чтобы убедиться, что вы выполняете ежедневные задачи мониторинга для своего решения IBM Spectrum Protect, ознакомьтесь с ежедневным контрольным списком для мониторинга.

Выполняйте ежедневные задачи мониторинга со страницы Обзор в компоненте Центр операций. Доступ к странице Обзор можно получить, открыв Центр операций и щелкнув по Обзоры.

На рисунке ниже показано расположение для завершения каждой операции.



Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте

Центр операций. В строке меню установите указатель мыши на значок параметров  и щелкните по Построитель команд.

В следующей таблице перечислены ежедневные задачи мониторинга и представлены инструкции по выполнению каждой задачи.

Табл. 1. Задачи ежедневного мониторинга

Задача	**Основные процедуры**	**Дополнительные процедуры и диагностическая информация**
Наблюдайте за уведомлениями о защите, которые могут указывать на атаку программы-вымогателя.	Если потенциальная атака программы-вымогателя обнаружена в среде IBM Spectrum Protect, то будет показано уведомление о защите на переднем плане Центр операций. Дополнительную информацию можно получить, щелкнув по сообщению, чтобы открыть страницу Уведомления о защите.	На странице Уведомления о защите можно выполнить следующие действия: • Просмотр подробностей уведомления по клиентам. Ограничение: В Центр операций версии 8.1.5, уведомления доступны только для клиентов резервного копирования-архивирования. • Подтвердите уведомление защиты, выбрав его и щелкнув по Подтвердить. При подтверждении уведомления о защите в столбец Подтверждение на странице Уведомления о защите добавляется символ галочки для выбранного клиента. Стандарт, по которому подтверждается уведомление, определяется в вашей организации. Галочка может означать, что вы исследовали проблему и решили, что это - ложное положительное. Это также может означать, что проблема существует, и она решается. • Назначьте уведомление о защите администратору, выбрав уведомление о защите и нажав Назначить. Чтобы рассмотреть назначение, администратор должен зарегистрироваться в Центр операций и щелкнуть Обзоры > Защита. Если вы не уверены, что администратор регулярно отслеживает страницу Уведомления о защите, сообщите администратору о назначении. • Если уведомление - ложное положительное, то можно выбрать уведомление о защите и щелкните по Сброс. Уведомление о защите удалено. Хронологические данные, используемые для базовых сравнений с самой последней операцией резервного копирования, удаляются. С этого момента вычисляется новая базовая линия.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
1 Определите, подвергаются ли клиенты риску оказаться незащищенными из-за неудавшихся или пропущенных операций резервного копирования.	Чтобы проверить, находятся ли клиенты под угрозой, в области Клиенты найдите уведомление Под угрозой. Чтобы просмотреть сведения, щелкните по области Клиенты. Внимание: Если процент Под угрозой намного больше обычного, то это может указывать на атаку программы-вымогателя. Атака программы-вымогателя может привести к сбоям резервного копирования, тем самым создавая риск для клиентов. Например, если процент клиентов в опасности обычно между 5% и 10%, но процент увеличивается до 40% или 50%, то изучите причину этого. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете увидеть и проанализировать ошибку клиента и запланировать журналы, выполнив следующие шаги: 1. В таблице Клиенты выберите клиент и щелкните по Сведения. 2. Чтобы диагностировать проблему, щелкните по Диагноз.	В случае клиентов, у которых нет установленной службы управления клиентом, получите доступ к системе клиента, чтобы проверить журналы ошибок клиента.
2 Определите, нужно ли уделить внимание ошибкам клиента или сервера.	Чтобы определить серьезность всех оповещений, о которых было сообщено, установите указатель мыши на столбцы в области Оповещения.	Чтобы увидеть дополнительную информацию об оповещениях, выполните следующие шаги: 1. Щелкните по области Оповещения. 2. В таблице Оповещения выберите оповещение. 3. В панели Журнал операций просмотрите сообщения. В панели показаны связанные сообщения, созданные до и после возникновения выбранного оповещения.
3 Определите, доступны ли серверы, которыми управляет Центр операций, для предоставления клиентам служб по защите данных.	1. Чтобы проверить, находятся ли серверы под угрозой, в области Серверы найдите уведомление Недоступен. 2. Чтобы увидеть дополнительную информацию, щелкните по области Серверы. 3. Выберите сервер в таблице Серверы и щелкните по Сведения.	Совет: Если вы обнаружите проблему, связанную со свойствами сервера, обновите свойства сервера: 1. В таблице Серверы выберите сервер и щелкните по Сведения. 2. Чтобы обновить свойства сервера, щелкните по Свойства.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
4 Определите, доступно ли достаточно пространства для перечня сервера, состоящего из базы данных сервера, активного журнала и архивного журнала.	1. Щелкните по области Серверы. 2. В столбце Состояние в таблице проверьте состояние сервера и устраните все ошибки: ◦ Нормальное Для базы данных сервера, активного журнала и архивного журнала доступен достаточный объем пространства. ◦ Критическое Для базы данных сервера, активного журнала или архивного журнала недостаточно пространства. Нужно немедленно добавить пространство, иначе работа служб защиты данных, предоставляемых сервером, будет прервана. ◦ Предупреждение , В базе данных сервера, активном журнале или архивном журнале заканчивается пространство. Если это условие повторяется, то нужно добавить пространство. ◦ Недоступно Невозможно получить состояние. Убедитесь, что сервер работает и что в сети нет ошибок. Это состояние показывается также, если ID администратора мониторинга заблокирован или недоступен на сервере по другой причине. Значение этого ID - IBM-OC-имя_хаб-сервера. ◦ Неотслеживаемый Неотслеживаемые серверы заданы на хаб-сервере, но не сконфигурированы для управления компонентом Центр операций. Чтобы сконфигурировать не отслеживаемый сервер, выберите сервер и щелкните по Отслеживать подчиненный.	Можно также просмотреть связанные оповещения на странице Оповещения. Дополнительную информацию об устранении ошибок смотрите в разделе Устранение проблем сервера.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
5 Проверьте операции резервного копирования базы данных.	Чтобы определить, когда в последний раз производилось резервное копирование сервера, выполните следующие шаги: 1. Щелкните по области Серверы. 2. В таблице Серверы проверьте столбец Последнее резервное копирование базы данных.	Чтобы получить более подробную информацию об операциях резервного копирования, выполните следующие шаги: 1. В таблице Серверы выберите строку и щелкните по Сведения. 2. В области Резервное копирование БД установите указатель мыши на галочки, чтобы прочесть информацию об операциях резервного копирования. Если резервное копирование базы данных не производилось недавно (например, за последние 24 часа), вы можете запустить операцию резервного копирования: 1. На странице Обзор в компоненте Центр операций щелкните по области Серверы. 2. В таблице выберите сервер и щелкните по Резервное копирование. Чтобы определить, сконфигурирована ли база данных сервера для автоматических операций резервного копирования, выполните следующие шаги: 1. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY DB: `query db f=d` 3. В выходной информации проверьте значение в поле `Полное имя класса устройств`. Если класс устройства указан, это означает, что сервер сконфигурирован для автоматического резервного копирования базы данных.
6 Отслеживайте другие задачи по обслуживанию сервера. Задачи по обслуживанию сервера могут включать в себя выполнение расписаний административных команд, сценариев обслуживания и связанных команды.	Чтобы найти информацию о процессах, которые завершились неудачно из-за проблем на сервере, выполните следующие шаги: 1. Выберите Серверы > Обслуживание. 2. Чтобы получить двухнедельную хронологию процесса, смотрите столбец Хронология. 3. Чтобы получить больше информации о запланированном процессе, установите указатель мыши на переключателее, связанном с процессом.	Более подробную информацию о процессах мониторинга и устранении проблем смотрите в электронной справке компонента Центр операций.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
7 Убедиться, что объем данных, переданных на серверы и полученных с них, находится в ожидаемом диапазоне.	• Чтобы получить обзор операций за последние 24 часа, смотрите область Операции. • Чтобы сравнить активность за последние 24 часа с активностью за предыдущие 24 часа, смотрите показатели в областях Текущие и Предыдущие.	• Если на сервер было отправлено больше данных, чем вы ожидали, определите, какие клиенты создают резервные копии большего объема данных, и исследуйте причину. Возможно, что дедупликация данных на стороне клиента работает неправильно. Внимание: Если объем резервных данных значительно больше обычного, то это может указывать на атаку программы-вымогателя. Когда программа-вымогатель шифрует данные, система обнаруживает, что данные изменяются и что резервная копия создается для измененных данных. Тем самым тома резервного копирования становятся больше. Чтобы узнать, какие клиенты затронуты, выберите вкладки Приложения, Виртуальные или Системы. • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.
8 Убедитесь, что пулы хранения доступны для резервного копирования данных клиента.	1. Если в области Хранение и доступность данных указаны проблемы, щелкните по Пулы, чтобы ознакомиться со сведениями: ○ Если показано состояние Критическое ⊗, это указывает на то, что в пуле хранения недостаточно доступного пространства или его состояние доступа - Недоступно. Внимание: Если состояние критическое, то изучите причину: ■ Если скорость дедупликации данных в пуле хранения значительно снижается, то это может указывать на атаку программы-вымогателя. Во время атаки программы-вымогателя данные шифруются и не могут дедуплицироваться. Чтобы проверить скорость дедупликации данных, в таблице Пулы хранения проверьте значение в столбце Процент экономии. ■ Если пул хранения неожиданно становится использован 100%, то это может указывать на атаку программы-	Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по Сведения.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
	вымогателя. Для проверки использования просмотрите значение в столбце Использованная емкость. Наведите мышь на значения, чтобы увидеть процент использованного и свободного пространства. ○ Если показано состояние Предупреждение ⚠, в пуле хранения заканчивается пространство или его состояние доступа - Только чтение. 2. Чтобы увидеть и используемое, свободное и общее пространство для выбранного пула хранения, установите указатель мыши над записями в столбце Использованная емкость.	
9 Убедитесь, что устройства хранения доступны для операций резервного копирования.	В области Хранение и доступность данных, в разделе Тома под столбцами емкости проверьте состояние, показанное рядом с элементом Устройства. Если для любого устройства показано состояние Критическое ⊗ или Предупреждение ⚠, исследуйте проблему. Чтобы просмотреть сведения, щелкните по Устройства.	Дисковые устройства могут находиться в критическом состоянии или в состоянии предупреждения по следующим причинам: • Для классов устройств DISK тома могут быть отключены или находиться в состоянии 'только для чтения'. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние томов. • Для классов устройств FILE, которые не используются совместно, могут быть отключены каталоги. Кроме того, для выделения чистых томов может оказаться недостаточно свободного пространства. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние каталогов. • Для классов устройств FILE, которые используются совместно, могут быть недоступны накопители. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. В других столбцах таблицы Дисковые устройства показано состояние накопителей и путей.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
10 Отслеживайте процессы репликации узла.	1. Чтобы узнать общее состояние процессов репликации узлов, смотрите область Репликации на странице Обзор в компоненте Центр операций. 2. Чтобы увидеть информацию о каждой паре реплицируемых серверов, щелкните по области Репликация. Внимание: Если вы замечаете неожиданное увеличение числа сбоев при репликации, то это может указывать на атаку программы-вымогателя. Изучите причину сбоев. 3. Чтобы узнать, какой объем данных был реплицирован за последние две недели и какова была скорость репликации, выберите пару серверов и щелкните по Сведения. 4. Чтобы увидеть информацию о репликации для клиента, щелкните по Клиенты на странице Обзор в компоненте Центр операций. Ознакомьтесь с данными в столбце Рабочая нагрузка репликации. Внимание: Если вы замечаете драматическое неожиданное увеличение нагрузки при репликации, то это может указывать на атаку программы-вымогателя. Изучите причину увеличенной нагрузки.	Чтобы выполнить расширенный мониторинг, прочтите информацию о запуске и завершении процессов репликации узлов, используя команды: 1. На странице Обзор компонента Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY REPLICATION. Инструкции смотрите в разделе QUERY REPLICATION (Запросить информацию о процессах репликации узлов). Если операция репликации была завершена успешно, значение `Всего файлов, подлежащих репликации` будет соответствовать значению `Всего реплицировано файлов`. Чтобы ознакомиться с сообщениями, связанными с процессом репликации узла на исходном сервере репликации или сервере репликации назначения, выполните следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Серверы. 2. Выберите исходный сервер репликации или сервер репликации назначения и щелкните по Сведения: ○ Чтобы увидеть активные задачи, щелкните по Активные задачи, выберите задачу и проверьте, показано ли состояние Выполняется. Подробные сведения смотрите в соответствующих журналах операций. ○ Чтобы увидеть выполненные задачи, щелкните по Выполненные задачи, выберите задачу и убедитесь, что показано состояние Выполнена. Подробные сведения смотрите в соответствующих журналах операций.

Контрольный список периодического мониторинга

Чтобы убедиться, что ваше решение работает правильно, выполните задачи в периодическом контрольном списке мониторинга. Запланируйте периодические задачи достаточно часто, чтобы вы могли обнаружить потенциальные неполадки, прежде чем они вызовут проблемы.

Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

Табл. 1. Задачи периодического мониторинга

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте производительность системы.	Определите, сколько времени требуется для операций резервного копирования клиента: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Найдите сервер, связанный с клиентом. 2. Щелкните по Серверы. Выберите сервер и щелкните по Сведения. 3. Чтобы увидеть продолжительность выполненных задач за последние 24 часа, щелкните по Выполненные задачи. 4. Чтобы увидеть продолжительность задач, выполненных более 24 часов тому назад, используйте команду QUERY ACTLOG. Следуйте инструкциям в разделе . 5. Если длительность операций резервного копирования клиента увеличивается при неясных причинах, исследуйте причину. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете диагностировать ошибки, влияющие на производительность, для клиента резервного копирования и архивирования, выполнив следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. 2. Выберите клиент резервного копирования и архивирования и щелкните по Сведения. 3. Чтобы получить журналы клиентов, щелкните по Диагностика.	Инструкции по сокращению времени, которое затрачивает клиент на резервное копирование данных на сервер, смотрите в разделе Устранение общих проблем, связанных с производительностью клиента. Ищите узкие места с точки зрения производительности. Инструкции смотрите в разделе Выявление узких мест производительности. Информацию о выявлении и устранении других проблем, отрицательно влияющих на производительность, смотрите в разделе Производительность.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите экономию дисков, обеспечиваемую дедупликацией данных.	1. Щелкните на странице Обзор в компоненте Центр операций по Пулы. 2. Выберите пул щелкните по Быстрый обзор. 3. В области Дедупликация данных смотрите сохраненную строку Пространство.	При расширенном мониторинге, чтобы получить подробную статистику процесса дедупликации данных для определенного пула хранения контейнеров каталогов или облачного пула хранения каталогов, выполните следующие шаги: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Получите статистический отчет, введя команду GENERATE DEDUPSTATS. Следуйте инструкциям в разделе GENERATE DEDUPSTATS (Сгенерировать статистику дедупликации данных для пула хранения каталога-контейнера). 3. Просмотрите статистический отчет, введя команду QUERY DEDUPSTATS. Следуйте инструкциям в разделе QUERY DEDUPSTATS (Запросить статистику дедупликации данных).

Убедитесь, что текущие файлы резервных копий для конфигурации устройств и информации о хронологии томов сохранены.	Получите доступ к расположениям хранения, чтобы убедиться, что файлы доступны. Предпочтительный метод заключается в том, чтобы сохранять файлы резервных копий в двум расположениях.
	Чтобы найти файлы хронологии томов и файлы конфигурации устройств, выполните следующие шаги:
	1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
	2. Чтобы найти файлы хронологии томов и конфигурации устройств, введите следующие команды:
	`query option volhistory`
	`query option devconfig`
	3. В выходной информации проверьте столбец Параметр опции, чтобы найти расположения файлов.
	Если произойдет бедствие, для восстановления базы данных сервера потребуется как файл хронологии томов, так и файл конфигурации устройств.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите, доступно ли достаточно пространства для файловой системы каталога экземпляра.	Убедитесь, что в файловой системе каталога экземпляра доступно, как минимум, 20% свободного пространства. Выполните действие, подходящее для вашей операционной системы: •  Операционные системы AIX Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -g` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Linux Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -h` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Windows В проводнике Windows щелкните правой кнопкой мыши по файловой системе и выберите Свойства. Проверьте информацию о емкости. Предпочтительное расположение каталога экземпляра зависит от операционной системы, в которой установлен сервер: •  Операционные системы AIX  Операционные системы Linux /home/tsminst1/tsminst1  Операционные системы Windows C:\tsminst1 Совет: Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Выявите неожиданную активность клиента.	Чтобы отслеживать операции клиента и определить, не превышает ли объем данных для томов ожидаемый объем, выполните следующие шаги: 1. На странице Обзор в компоненте Центр операций щелкните по области Клиенты. 2. Чтобы увидеть операции за посредние две недели, дважды щелкните по любому клиенту. 3. Чтобы узнать число байт, отправленных клиенту, щелкните по вкладке Свойства. 4. В области Последний сеанс проверьте строку Отправлено клиенту.	Когда вы дважды щелкнете по клиенту в таблице Клиенты, в области Операции за 2 недели будет показан объем данных, которые клиент каждый день отправлял на сервер. Регулярно проверяйте SQL-таблицу сводной информации о деятельности, содержащую статистические данные о клиентских сеансах. Чтобы сравнить текущие операции с предыдущими, воспользуйтесь оператором SQL SELECT. Если уровень операций существенно отличается от предыдущего, то это может указывать на атаку программы-вымогателя. Регулярно проверяйте журнал операций. Найдите сообщения ANE, указывающие, для скольких файлов созданы резервные копии и выполнена инспекция. Сравните текущие данные о скорости дедупликации с прежней скоростью. Если в созданной резервной копии необычно много файлов или уровень дедупликации данных неожиданно спадает до 0, то это может указывать на атаку программы-вымогателя

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте рост пула хранения с течением времени.	1. На странице Обзор в компоненте Центр операций щелкните по области Пулы. 2. Чтобы увидеть емкость, используемую за последние две недели, выберите пул и щелкните по Сведения.	Советы: • Чтобы задать период времени, который должен пройти, прежде чем из пула хранения каталогов-контейнеров или пула хранения облачных контейнеров будут удалены все дедуплицированные экстенты, после того как на них не появлялось никаких ссылок в перечне, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. 3. Задайте длительность в поле `Период задержки для повторного использования контейнера`. • Чтобы определить производительность дедупликации данных для пулов хранения каталогов-контейнеров и облачных контейнеров, используйте команду GENERATE DEDUPSTATS. • Чтобы просмотреть статистику дедупликации данных для пула хранения, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. Либо используйте команду QUERY EXTENTUPDATES, чтобы увидеть информацию об обновлениях экстентов данных в пулах хранения каталогов-контейнеров или облачных контейнеров. Выходная информация команды может помочь вам определить, на какие экстенты данных уже нет ссылок и какие из них подлежат удалению из системы. В выходной информации смотрите, какое число экстентов данных подлежит удалению из системы. Этот показатель напрямую коррелируется с объемом свободного пространства, которое будет доступно в пуле хранения контейнера. • Чтобы увидеть объем физического пространства, занятого файловым пространством после удаления экономии за счет дедупликации данных, используйте команду select * from occupancy. В выходной информации команды будет содержаться значение LOGICAL_MB. LOGICAL_MB - это объем, используемый этим файловым пространством.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Оцените временные характеристики расписаний клиента. Убедитесь, что начальное и конечное время расписаний клиентов соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Клиенты > Расписания. В таблице Расписания в столбце Запуск показано сконфигурированное время запуска для запланированной операции. Чтобы увидеть, когда была запущена самая последняя операция, установите указатель мыши на значок часов.	Совет: Если операция клиента выполняется дольше, чем ожидается, вы можете получить сообщение с предупреждением. Сделайте следующее: 1. На странице обзора в компоненте Центр операций установите указатель мыши на Клиенты и щелкните по Расписания. 2. Выберите расписание и щелкните по Сведения. 3. Просмотрите сведения о расписании, щелкнув по синей стрелке рядом со строкой. 4. В поле Оповещение среды выполнения задайте время, когда будет выдано сообщение с предупреждением, если запланированная операция не будет выполнена. 5. Щелкните по Сохранить.
Оцените временные характеристики задач по обслуживанию. Убедитесь, что начальное и конечное время задач по обслуживанию соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Серверы > Обслуживание. В таблице Обслуживание проверьте информацию в столбце Время последнего выполнения. Чтобы увидеть, когда была запущена самая последняя задача по обслуживанию, установите указатель мыши на значок часов.	Совет: Если задача по обслуживанию выполняется слишком долго, измените начальное время или максимальное время выполнения. Сделайте следующее: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров  и щелкните по Построитель команд. 2. Чтобы изменить время запуска или максимальное время выполнения задачи, введите команду UPDATE SCHEDULE. Инструкции смотрите в разделе UPDATE SCHEDULE (Изменить запланированное задание клиента).

Ссылки, связанные с данной:

QUERY ACTLOG (Запросить информацию журнала операций)

UPDATE STGPOOL (обновить пул хранения)

QUERY EXTENTUPDATES (Запросить обновленные экстенты данных)

Проверка на соответствие лицензии

Убедитесь, что ваше решение IBM Spectrum Protect соответствует положениям вашего лицензионного соглашения. Регулярно производя мониторинг решения, можно отслеживать тенденции роста данных или использование единиц мощности процессора (processor value unit, PVU). Используйте эту информацию, чтобы спланировать будущее приобретение лицензий.

Об этой задаче

Метод, который вы используете, чтобы убедиться, что ваше решение соответствует условиям лицензии, зависит от положений вашего лицензионного соглашения IBM Spectrum Protect.

Фронтальное лицензирование мощности

Фронтальная модель определяет требования к лицензии на основе объема первичных данных, о которых клиентами было сообщено, что для них создавались резервные копии. К клиентам относятся приложения, виртуальные машины и компьютеры.

Внутреннее лицензирование мощности

Внутренняя модель определяет требования к лицензии на основе числа терабайт данных, которые хранятся в первичных пулах хранения и репозиториях.

Советы:

- Чтобы обеспечить точность оценки фронтальной и внутренней емкости, установите новейшую версию программы клиента на каждом клиентском узле.
- Информация о фронтальной и внутренней емкости в Центр операций предназначена только для планирования и оценки.

Лицензирование PVU

Модель PVU основана на использовании PVU серверными устройствами.

Важное замечание: Расчеты PVU, выполняемые IBM Spectrum Protect, считаются оценочными и не имеют юридической силы. Информация о лицензировании PVU, сообщенная продуктом IBM Spectrum Protect, не рассматривается как допустимая замена для IBM® License Metric Tool.

Самую последнюю информацию о моделях лицензирования смотрите в информации о продукте и лицензии на веб-сайте семейства продуктов IBM Spectrum Protect. Если у вас возникнут вопросы или замечания, касающиеся требований по лицензированию, обращайтесь к вашему поставщику программы IBM Spectrum Protect.

Процедура

Чтобы отследить соответствие лицензии, выполните шаги, соответствующие положениям вашего лицензионного соглашения.

Совет: Центр операций обеспечивает электронный отчет, в котором просуммировано использование фронтальной и внутренней емкости. Отчеты можно автоматически регулярно отправлять одному или нескольким получателям. Чтобы сконфигурировать электронные отчеты и управлять ими, щелкните по Отчеты в строке меню Центр операций.

Опция	Описание
Фронтальная модель	a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. На странице Фронтальное использование показана оценка фронтальной емкости. b. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости. c. Чтобы оценить емкость для клиентов, которые не сообщают об использовании емкости, перейдите на следующий FTP-сайт, где представлены инструменты измерения и инструкции: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Чтобы изменить фронтальную емкость в соответствии со сценарием, выполните инструкции в самом последнем доступном руководстве по лицензированию. d. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария. e. Убедитесь, что оценка емкости соответствует вашему лицензионному соглашению.
Внутренняя модель	Ограничение: Если исходный и целевой серверы репликации не используют одни и те же параметры политики, вы не сможете использовать Центр операций для мониторинга использования внутренней емкости для реплицируемых клиентов. Информацию о том, как оценить использование емкости для этих клиентов, смотрите в следующей публикации technote 1656476. a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. b. Щелкните по вкладке Внутренний. c. Проверьте, соответствует ли оценка объема данных вашему лицензионному соглашению.

Опция	Описание
Модель PVU	Иформацию о том, как оценить соответствие условиям лицензирования PVU, смотрите в разделе Оценка соответствия модели лицензирования PVU.

Состояние системы отслеживания с использованием отчетов по электронной почте

Настройте компонент Центр операций, чтобы сгенерировать отчеты по электронной почте, в которых суммируется состояние системы. Вы можете сконфигурировать соединение с почтовым сервером, изменить параметры отчета и (необязательно) создать пользовательские отчеты.

Прежде чем начать

Прежде чем настраивать отчеты по электронной почте, убедитесь, что выполнены следующие требования:

- Доступен хост-сервер Simple Mail Transfer Protocol (SMTP) для отправки и получения отчетов по электронной почте. Сервер SMTP должен быть сконфигурирован как открытый почтовый ретранслятор. Вы также должны убедиться, что у сервера IBM Spectrum Protect, который отправляет сообщения электронной почты, есть доступ к серверу SMTP. Если центр операций установлен на отдельном компьютере, этому компьютеру не требуется доступ к серверу SMTP.
- Чтобы задавать отчеты по электронной почте, нужно иметь системные полномочия для сервера.
- Чтобы задать получателей, можно ввести один или несколько адресов электронной почты или ID администраторов. Если вы собираетесь ввести ID администратора, ID должен быть зарегистрирован на хаб-сервере и с ним должен быть связан адрес электронной почты. Чтобы задать адрес электронной почты для администратора, используйте параметр EMAILADDRESS в команде UPDATE ADMIN.

Об этой задаче

Вы можете сконфигурировать Центр операций для отправки отчета об общих операциях, отчета о соответствии лицензии, а также одного или нескольких пользовательских отчетов. Вы создаете пользовательские отчеты, выбирая шаблоны из набора обычно используемых шаблонов отчетов или вводя операторы SQL SELECT, чтобы запросить информацию на управляемых серверах.

Процедура

Чтобы настроить электронные отчеты и управлять ими, сделайте следующее:

1. В строке меню компонента Центр операций выберите Отчеты.
2. Если соединение с сервером электронной почты еще не сконфигурировано, щелкните по Сконфигурировать почтовый сервер и заполните поля. После того как вы сконфигурируете почтовый сервер, будут включены отчет об общих операциях и отчет о соответствии лицензии.
3. Чтобы изменить параметры отчета, выберите отчет, щелкните по Сведения и обновите форму.
4. Необязательно: Чтобы добавить пользовательский отчет, щелкните по + Отчет и заполните поля.
   Совет: Чтобы сразу же запустить и отправить отчет, выберите отчет и нажмите на Отправить.

Результаты

Разрешенные отчеты будут отправлены в соответствии с заданными параметрами.
Ссылки, связанные с данной:
UPDATE ADMIN (обновление администратора)

Управление операциями для дискового решения с несколькими площадками

Используйте эту информацию для управления операциями при дисковом решении для нескольких площадок с IBM Spectrum Protect, включающим в себя сервер и использующим дедупликацию данных для нескольких площадок.

- Управление Центром операций
  Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.
- Защита приложений, виртуальных машин и компьютеров
  Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.
- Управление хранилищем данных
  Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.
- Управление репликацией
  Используйте репликацию для восстановления данных на площадке восстановления после аварии и для поддержания одного уровня файлов на серверах источника и назначения. Вы можете управлять репликацией на уровне узлов. Вы также можете защитить данные на уровне пула хранения.
- Защита сервера
  Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.
- Остановка и запуск сервера
  Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.
- Планирование обновления сервера
  Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.
- Подготовка к отключению или обновлению системы
  Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.
- Реализация плана аварийного восстановления
  Примените стратегию аварийного восстановления, чтобы восстановить приложения, если произойдет авария, и обеспечить высокую доступность сервера.
- Восстановление от потери данных или системных отключений электричества
  Вы можете восстановить данные IBM Spectrum Protect, которые были утрачены, когда произошла авария или системный перебой в питании. Можно восстановить пулы хранения каталогов-контейнеров, данные клиентов и базы данных.

Управление Центром операций

Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.

- Добавление и удаление подчиненных серверов
  В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.
- Запуск и остановка веб-сервера
  Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.
- Перезапуск мастера начального конфигурирования
  Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.
- Изменение хаб-сервера
  Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.
- Восстановление конфигурации до предварительно сконфигурированного состояния
  При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Добавление и удаление подчиненных серверов

В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

Об этой задаче

Подчиненные серверы отправляют оповещения и информацию о состоянии хаб-серверу. Центр операций содержит консолидированное представление оповещений и информации о состоянии для хаб-сервера и всех подчиненных серверов.

- Добавление подчиненного сервера
  После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.
- Удаление подчиненного сервера
  Можно удалить подчиненный сервер из Центра операций.

Добавление подчиненного сервера

После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.

Прежде чем начать

Связь между подчиненным сервером и хаб-сервером должна быть защищена с использованием протокола Transport Layer Security (TLS). Для защиты связи добавьте сертификат подчиненного сервера в файл доверенных сертификатов хаб-сервера.

Процедура

1. Щелкните в панели меню Центр операций по Серверы. Откроется страница Серверы.

   В таблице на странице Серверы состоянием сервера может быть "Не отслеживается" Это состояние означает, что хотя администратор и определил этот сервер на хаб-сервере при помощи команды DEFINE SERVER, этот сервер еще не сконфигурирован в качестве подчиненного сервера.

2. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по Отслеживать подчиненный.
   - Если сервера, который вы хотите добавить, нет в таблице, а защищенная связь SSL/TLS не требуется, то щелкните по + Подчиненный в панели меню таблицы.
3. Задайте нужную информацию и выполните действия в мастере конфигурирования подчиненных серверов.
   Совет: Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как подчиненный сервер.

Удаление подчиненного сервера

Можно удалить подчиненный сервер из Центра операций.

Об этой задаче

Вам может потребоваться удалить подчиненный сервер, например, в следующих ситуациях:

- Вы хотите переместить подчиненный сервер с одного хаб-сервера на другой.
- Подчиненный сервер больше не нужен.

Процедура

Чтобы удалить подчиненный сервер из группы серверов, которая управляется хаб-сервером, сделайте следующее:

1. В командной строке IBM Spectrum Protect введите следующую команду для хаб-сервера:

   ```
   QUERY MONITORSETTINGS
   ```

2. Скопируйте в выходных результатах команды имя, указанное в поле Отслеживаемые группы.
3. Введите на хаб-сервере следующую команду, где *имя_группы* - это имя отслеживаемой группы, а *имя_члена* - это имя подчиненного сервера.

   ```
   DELETE GRPMEMBER имя_группы имя_члена
   ```

4. Необязательно: Если вы хотите переместить подчиненный сервер с одного хаб-сервера на другой, **не** выполняйте этот шаг. В ином случае можно запретить оповещения и мониторинг для подчиненного сервера, введя на подчиненном сервере следующие команды:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Необязательно: Если определение подчиненного сервера используется в других целях, например, для конфигурирования предприятия, маршрутизации команд, хранения виртуальных томов или управления библиотекой, **не** выполняйте этот шаг. В противном случае можно удалить определение подчиненного сервера на хаб-сервере, введя на хаб-сервере следующую команду:

   ```
   DELETE SERVER имя_подчиненного_сервера
   ```

   Совет: Если определение сервера удаляется сразу же после удаления сервера из отслеживаемой группы, информация о состоянии сервера может остаться в центре операций на неопределенно долгое время.

   Чтобы избежать этой проблемы, перед удалением определения сервера дождитесь, когда пройдет интервал сбора состояния. Интервал сбора данных состояния показан на странице Параметры в центре операций.

Запуск и остановка веб-сервера

Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.

Процедура

1. Остановите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./stopserver.sh
     ```

   - Операционные системы LinuxВведите следующую команду:

     ```
     service opscenter.rc stop
     ```

   - Операционные системы WindowsВ окне Службы остановите службу Центр операций IBM Spectrum Protect.
2. Запустите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./startserver.sh
     ```

   - Операционные системы LinuxВведите следующие команды:

     Запустите сервер:

     ```
     service opscenter.rc start
     ```

     Перезапустите сервер:

     ```
     service opscenter.rc restart
     ```

     Определите, работает ли сервер:

     ```
     service opscenter.rc status
     ```

- Операционные системы WindowsВ окне Службы запустите службу Центр операций IBM Spectrum Protect.

Перезапуск мастера начального конфигурирования

Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.

Прежде чем начать

Чтобы изменить следующие параметры, используйте страницу Параметры в Центр операций вместо перезапуска мастера начального конфигурирования:

- Периодичность обновления данных
- Интервал времени, в течение которого предупреждение активно, неактивно или закрывается
- Условия, обозначающие риск для клиентов

Центр операций помогает включить дополнительную информацию о том, как изменить эти параметры.

Об этой задаче

Для перезапуска мастера начального конфигурирования необходимо удалить файл свойств с информацией о соединении с хаб-сервером. Однако никакие настройки оповещений, мониторинга, состояния 'Под угрозой' или среды для нескольких серверов, заданные для хаб-сервера, не удаляются. Эти настройки используются как настройки мастера конфигурирования по умолчанию при его перезапуске.

Процедура

1. Остановите веб-сервер Центр операций.
2. На компьютере с установленным продуктом Центр операций перейдите в следующий каталог, где *каталог_установки* представляет собой каталог, в котором установлен продукт Центр операций:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer

   Например:
   - Операционные системы AIXОперационные системы Linux/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windowsc:\Program Files\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Удалите из каталога guiServer файл serverConnection.properties.
4. Запустите веб-сервер Центра операций.
5. Откройте Центр операций.
6. Переконфигурируйте Центр операций при помощи мастера конфигурирования. Задайте новый пароль для ID администратора мониторинга.
7. На каждом из подчиненных серверов, ранее связанных с хаб-сервером, измените пароль для ID администратора мониторинга, введя следующую команду в интерфейсе командной строки IBM Spectrum Protect:

   ```
   UPDATE ADMIN  IBM-OC-имя_хаб-сервера новый_пароль
   ```

   Ограничение: Не изменяйте никакие другие параметры для этого ID администратора. После того, как задан начальный пароль, он автоматически управляется Центр операций.

Изменение хаб-сервера

Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.

Процедура

1. Перезапустите мастер начального конфигурирования Центр операций. При выполнении этой процедуры вы удаляете соединение хаб-сервера.
2. При помощи мастера сконфигурируйте Центр операций для соединения с новым хаб-сервером.

Задачи, связанные с данной:
Перезапуск мастера начального конфигурирования

Восстановление конфигурации до предварительно сконфигурированного состояния

При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Процедура

Чтобы восстановить конфигурацию, выполните следующие шаги:

1. Остановите веб-сервер Центр операций.
2. Деконфигурируйте хаб-сервер, выполнив следующие действия:
   a. Введите на хаб-сервере следующие команды:

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-имя_хаб-сервера
      ```

      Совет: `IBM-OC-`*`имя_хаб-сервера`* - это ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Переустановите пароль для хаб-сервера, введя на хаб-сервере следующую команду:

      ```
      SET SERVERPASSWORD ""
      ```

      Внимание: Не выполняйте этот шаг, если хаб-сервер сконфигурирован с другими серверами для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.
3. Отмените конфигурацию всех подчиненных серверов, выполнив следующие шаги:
   a. Чтобы определить, остаются ли какие-либо подчиненные серверы как члены группы серверов, введите на хаб-сервере следующую команду:

      ```
      QUERY SERVERGROUP IBM-OC-имя_хаб-сервера
      ```

      Совет: `IBM-OC-`*`имя_хаб-сервера`* - это имя отслеживаемой группы серверов, которая была автоматически создана при конфигурировании первого подчиненного сервера. Это имя группы серверов - это также ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Чтобы удалить из группы серверов подчиненные серверы, введите на хаб-сервере следующую команду для каждого подчиненного сервера:

      ```
      DELETE GRPMEMBER IBM-OC-имя_хаб-сервера имя_подчиненного_сервера
      ```

   c. После удаления всех подчиненных серверов из группы серверов введите следующую команду на хаб-сервере:

      ```
      DELETE SERVERGROUP IBM-OC-имя_хаб-сервера
      SET MONITOREDSERVERGROUP ""
      ```

   d. Введите на каждом подчиненном сервере следующую команду:

      ```
      REMOVE ADMIN IBM-OC-имя_хаб-сервера
      SETOPT PUSHSTATUS NO
      SET ALERTMONITOR OFF
      SET STATUSMONITOR OFF
      ```

   e. Удалите на каждом из подчиненных серверов определение хаб-сервера, введя на серверах следующую команду:

      ```
      DELETE SERVER имя_хаб_сервера
      ```

      Внимание: Не выполняйте этот шаг, если данное определение используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.
   f. Удалите на хаб-сервере определение каждого из подчиненных серверов, введя следующую команду:

      ```
      DELETE SERVER имя_подчиненного_сервера
      ```

Внимание: Не выполняйте этот шаг, если данное определение сервера используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.

4. Восстановите параметры по умолчанию для каждого сервера, введя следующие команды:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Перезапустите мастер начального конфигурирования Центр операций.

Задачи, связанные с данной:
Перезапуск мастера начального конфигурирования
Запуск и остановка веб-сервера

Защита приложений, виртуальных машин и компьютеров

Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.

- Добавление клиентов
  После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.
- Управление операциями клиентов
  Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.
- Управление обновлениями клиентов
  Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).
- Списание клиентского узла
  Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).
- Деактивация данных для высвобождения пространства хранения
  В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Добавление клиентов

После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.

Об этой задаче

Процедура описывает базовые шаги по добавлению клиента. Более конкретные инструкции по конфигурированию клиентов смотрите в документации по продукту, который вы установили на клиентском узле. У вас могут быть следующие типы клиентских узлов:

Клиентские узлы приложений
К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Системные клиентские узлы
: К системным клиентским узлам относятся рабочие станции, файл-серверы сетевого хранилища данных (NAS) и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Процедура

Чтобы добавить клиент, сделайте следующее:

1. Выберите программу, которую нужно установить на клиентском узле, и спланируйте установку. Следуйте инструкциям в разделе Выбор программного обеспечения клиента и планирование установки.
2. Укажите, как следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе Как задать роли для резервного копирования и архивирования данных клиента.
3. Укажите, когда следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе Планирование операций резервного копирования и архивирования.
4. Чтобы позволить клиенту соединяться с сервером, зарегистрируйте клиент. Следуйте инструкциям в разделе Регистрация клиентов.
5. Чтобы начать защищать клиентский узел, установите и сконфигурируйте выбранную программу на клиентском узле. Следуйте инструкциям в разделе Установка и настройка клиентов.

Выбор программного обеспечения клиента и планирование установки

Для разных типов данных требуются разные типы защиты. Определите, какой тип данных вам нужно защищать, и выберите соответствующую программу.

Об этой задаче

Предпочтительная практика заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить демон приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, вы должны следовать инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Процедура

В зависимости от ваших целей выберите продукты, которые нужно установить, и ознакомьтесь с инструкциями по установке.
Совет: Если вы установите программу-клиент сейчас, вы, прежде чем сможете использовать клиент, также должны будете выполнить задачи по конфигурированию клиента, описанные в разделе Установка и настройка клиентов.

Цель	Продукт и описание	Инструкции по установке

Цель	Продукт и описание	Инструкции по установке
Защитить файл-сервер или рабочую станцию	Клиент резервного копирования и архивирования производит резервное копирование и архивирование файлов и каталогов с файл-серверов и рабочих станций в хранилище. Вы также можете восстанавливать и получать версии резервных копий и архивные копии файлов.	• Требования клиента резервного копирования и архивирования • Установить клиентов резервного копирования и архивирования UNIX и Linux • Первая установка клиента Windows
Защитить приложения с использованием резервного копирования снимков и возможностей восстановления	IBM Spectrum Protect Snapshot защищает данные с использованием интегрированного резервного копирования снимков и возможностей восстановления с учетом информации о приложениях. Вы можете защитить данные, которые хранятся в приложениях IBM программное обеспечение баз данных DB2 и SAP, Oracle, Microsoft Exchange и Microsoft SQL Server.	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
Защитить приложение электронной почты на сервере IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов IBM Domino.	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0)
Защитить приложение электронной почты на сервере Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов Microsoft Exchange.	Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Защитить базу данных IBM DB2	Интерфейс прикладного программирования (API) можно использовать для резервного копирования данных DB2 на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных IBM Informix	API клиента резервного копирования и архивирования можно использовать для резервного копирования данных Informix на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных Microsoft SQL	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server защищает данные Microsoft SQL.	Установка Data Protection for SQL Server в ядре сервера Windows
Защитить базу данных Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle защищает данные Oracle.	Установка Data Protection for Oracle
Защитить среду SAP	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP обеспечивает защиту, настроенную для сред SAP. Продукт предназначен для того, чтобы повышать доступность серверов базы данных SAP и сокращать рабочую нагрузку администрирования.	• Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

Цель	Продукт и описание	Инструкции по установке
Защитить виртуальную машину	IBM Spectrum Protect for Virtual Environments обеспечивает защиту, настроенную для виртуальных сред Microsoft Hyper-V и VMware. IBM Spectrum Protect for Virtual Environments можно использовать для создания постоянных инкрементных резервных копий, хранящихся на централизованном сервере, создания политик резервного копирования и восстановления виртуальных машин или отдельных файлов. Либо используйте клиент резервного копирования и архивирования, чтобы производить резервное копирование и восстановление полной виртуальной машины VMware или Microsoft Hyper-V. Можно также производить резервное копирование и восстановление файлов или каталогов с виртуальной машины VMware.	• Установка Data Protection for Microsoft Hyper-V • Установка и обновление Data Protection for VMware • Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)

Совет: Чтобы использовать клиент для управления пространством, можно установить IBM Spectrum Protect for Space Management или IBM Spectrum Protect HSM for Windows.

Как задать роли для резервного копирования и архивирования данных клиента

Прежде чем вы добавите клиент, убедитесь, что соответствующие правила определены для поддержки и архивирования клиентских данных. В ходе процесса регистрации клиента вы назначается клиентский узел в домен политики, в котором есть правила, управляющие тем, как и когда производится сохранение данных клиента.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с политиками, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Планирование операций резервного копирования и архивирования.
- Если вы не знакомы с политиками, то выполните шаги в этой процедуре.

Об этой задаче

Политики влияют на то, какой объем данных хранится в течение долгого времени и сколько времени данные сохраняются и будут доступны клиентам для восстановления. Для достижения целей для защиты данных можно обновить политику по умолчанию и создать собственные политики. Политика включает следующие правила:

- Как и когда производится резервное копирование и архивирование файлов в серверное хранилище.
- Число копий файла и время хранения копий в серверном хранилище.

В ходе процесса регистрации клиента вы назначается клиент в *домен политики*. Политика для отдельного клиента определяется правилами в домене политики, который назначен для клиента. В домене политики действующие правила находятся в активном *наборе политик*.

Когда клиент копирует или архивирует файл, файл привязывается к классу управления в активном наборе политик домена политики. *Класс управления* - это ключевой набор правил для управления данными клиента. Операции резервного копирования и архивирования на клиенте используют настройки в классе управления по умолчанию домена политики, если вы далее не настраиваете политику. Политику можно настроить, задав больше классов управления и назначив их использование через опции клиента.

Опции клиента можно задать в локальном, доступном для изменения файле в системе клиента и в наборе опций клиента на сервере. Опции в наборе опций клиента на сервере могут переопределять локальный файл опций клиента или могут добавлять в него опции.

Процедура

1. Ознакомьтесь с политиками, сконфигурированными для вашего решения - следуйте инструкциям в разделе Просмотр политик.
2. Если необходимо внести незначительные изменения для соответствия требованиям хранения данных, следуйте инструкциям в разделе Изменение политик.
3. Необязательно: Если вам нужно создать домены политики или внести расширенные изменения в политики, чтобы выполнить требования к хранению данных, смотрите раздел Настройка политик.

Просмотр политик

Просмотрите политики, чтобы определить, не нужно ли их изменить в соответствии с вашими требованиями.

Процедура

1. Чтобы просмотреть активный наборов политик для домена политики, сделайте следующее:
   a. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
   b. На странице Сводка для домена политики щелкните по вкладке Наборы политики.
   Совет: Чтобы облегчить возможность восстановления данных после атаки программы-вымогателя, следуйте инструкциям ниже:
      - Убедитесь, что значение в столбце Резервные копии - это минимум 2. Предпочтительное значение - 3, 4 или более.
      - Убедитесь, что значение в столбце Сохранять дополнительные резервные копии - это минимум 14 дней. Предпочтительное значение равно 30 или более дням.
      - Убедитесь, что значение в столбце Сохранять архивы - это минимум 30 дней.

   Если программа IBM Spectrum Protect for Space Management установлена на клиенте, то убедитесь, что создана резервная копия данных, перед тем как перемещать данные. В команде DEFINE MGMTCLASS или UPDATE MGMTCLASS задайте MIGREQUIRESBKUP=YES. Далее следуйте руководящим подсказкам.
2. Для просмотра бездействующих наборов политики для домена политики сделайте следующее:
   a. На странице Наборы политик щелкните по Конфигурировать. Теперь можно просмотреть и изменить неактивные наборы политики.
   b. Прокрутите неактивные наборы политик, используя стрелки Вперед и Назад. При просмотре неактивного набора политики параметры, которые отличают этот неактивный набор политик от активного набора политик, будут выделены.
   c. Щелкните по переключателю Конфигурировать. Теперь наборы политик больше нельзя изменять.

Изменение политик

Чтобы изменить правила, применимые к домену политики, измените активный набор политик для домена политики. Можно также активировать для домена другой набор политик.

Прежде чем начать

Изменения политики могут повлиять на хранение данных. Убедитесь, чтобы вы продолжаете резервное копирование данных, имеющих существенное значение для вашей организации, чтобы можно было восстановить эти данные, если произойдет бедствие. Также убедитесь, что в вашей системе достаточно пространства хранения для запланированных операций резервного копирования.

Об этой задаче

Вы изменяете набор политик, изменяя один или несколько классов управления в наборе политик. Если вы измените активный набор политик, изменения не будут доступны клиентам, пока вы не активируете повторно набор политик. Чтобы сделать измененный набор политик доступным клиентам, активируйте набор политик.

Хотя для домена политики можно задать несколько наборов политик, активным может быть только один набор политик. При активации другого набора политики он заменяет активный в данный момент набор политик.

Предпочтительный опыт определения политик описан в разделе Настройка политик.

Процедура

1. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики.

   На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.

3. Щелкните по переключателю Конфигурировать. Набор политик доступен для изменения.
4. Необязательно: Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
5. Измените набор политик, выполнив любое из следующих действий:

Опция	Описание
Добавьте класс управления	a. В таблице Наборы политик щелкните по +Класс управления. b. Чтобы задать правила для резервного копирования и архивирования данных, заполните поля в окне Добавить класс управления. c. Чтобы сделать класс управления классом управления по умолчанию, включите переключатель Сделать значением по умолчанию. d. Щелкните по Добавить.
Удалите класс управления	В столбце Класс управления щелкните по -. Совет: Чтобы удалить класс управления по умолчанию, нужно сначала назначить другой класс управления классом управления по умолчанию.
Сделать класс управления классом управления по умолчанию	Щелкните по радиокнопке в столбце Значение по умолчанию для класса управления. Совет: Класс управления по умолчанию управляет файлами клиента, если для файла не назначен другой класс управления или если класс управления файла не подходит для управления файлом. Чтобы убедиться в том, что клиенты всегда могут производить резервное копирование и архивирование файлов, выберите класс управления по умолчанию и для резервного копирования, и для архивирования файлов.
Изменить класс управления	Чтобы изменить свойства класса управления, обновите поля в таблице.

6. Щелкните по Сохранить.
   Внимание: При активации нового набора политик можно потерять данные. Данные, защищенные в соответствии с одним набором политик, могут оказаться незащищенными с точки зрения другого набора политик. Поэтому, прежде чем активировать набор политик, убедитесь, что разница между предыдущим набором политик и новым набором политик не вызовет потерю данных.
7. Выберите Активировать. Будет показана сводка различий между активным набором политик и новым набором политик. Убедитесь, что изменения в новом наборе политики совместимы с вашими требованиями к хранению данных; для этого выполните следующие шаги:
   a. Проверьте различия между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном наборе политик, будут связаны с классами управления с теми же именами в новом наборе политик.
   b. Укажите в активном наборе политики классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут управляться классом управления по умолчанию в новом наборе политик.
   c. Если изменения, которые должны быть реализованы набором политики, являются допустимыми, выберите переключатель Я понимаю, что эти обновления могут вызвать потерю данных и щелкните по Активировать.

Планирование операций резервного копирования и архивирования

Прежде чем зарегистрировать новый клиент на сервере, убедитесь, что существует расписание, позволяющее указать, когда выполняются операции резервного копирования и архивирования. В процессе регистрации можно назначить расписание клиенту.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с расписаниями, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Регистрация клиентов.
- Если вы не знакомы с расписаниями или расписания нужно изменить, выполните шаги в этой процедуре.

Об этой задаче

Как правило, операции резервного копирования для всех клиентов должны выполняться ежедневно. Спланируйте рабочую нагрузку клиента и сервера, чтобы обеспечить наивысшую производительность для вашей среды хранения. Чтобы избежать перекрывания операций клиента и сервера, рассмотрите возможность запланировать выполнение операций резервного копирования и архивирования клиента по ночам. Если операции клиента и сервера будут перекрываться или для их обработки не выделят достаточно времени и ресурсов, то вы можете столкнуться со снижением производительности системы, неудачным завершением операций и другими проблемами.

Процедура

1. Проверьте доступные расписания, установив указатель мыши на Клиенты в строке меню Центр операций. Щелкните по Расписания.
2. Необязательно: Измените или создайте расписание, выполнив следующие шаги:

Опция	Описание
Изменение расписания	a. В представлении Расписания выберите расписание и щелкните по Сведения. b. На странице Сведения о расписании просмотрите сведения, щелкнув по синим стрелкам в начале строк. c. Измените параметры в расписании и нажмите на Сохранить.
Создание расписания	В представлении Расписания щелкните по +Расписание и выполните шаги по созданию расписания.

3. Необязательно: Чтобы сконфигурировать параметры расписания, которые не видны в компоненте Центр операций, используйте серверную команду. Например, вы можете счесть целесообразным запланировать операцию клиента, которая создает резервную копию определенного каталога и назначает для него класс управления, отличающийся от класса управления по умолчанию.
   a. На странице Обзор в компоненте Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
   b. Введите команду DEFINE SCHEDULE, чтобы создать расписание, или команду UPDATE SCHEDULE, чтобы изменить расписание. Дополнительные сведения о командах смотрите в разделах DEFINE SCHEDULE (определение расписания выполнения административных команд) или UPDATE SCHEDULE (Изменить запланированное задание клиента).

Задачи, связанные с данной:
Настройка расписания для ежедневных операций

Регистрация клиентов

Зарегистрируйте клиент, чтобы убедиться, что он может соединиться с сервером, а сервер может защитить данные клиента.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию technote 7048963.
Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе Аутентификация пользователей с использованием базы данных Active Directory.

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды REGISTER NODE и задайте параметр USERID:

  ```
  register node имя_узла пароль userid=имя_узла
  ```

  где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе Регистрация узла.
- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центр операций. Сделайте следующее:
  a. В панели меню Центра операций выберите Клиенты.
  b. В таблице Клиенты щелкните по + Клиент.
  c. Выполните шаги в мастере Добавить клиент:
     i. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель Включить в области Дедупликация данных на стороне клиента.
     ii. В окне Конфигурация скопируйте значения TCPSERVERADDRESS, TCPPORT, NODENAME, и DEDUPLICATION.
     Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
     iii. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     iv. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     v. Щелкните по Добавить клиент.

Ссылки, связанные с данной:
Опция Tcpserveraddress
Опция Tcpport
Опция Nodename
Опция дедупликации

Установка и настройка клиентов

Чтобы начать защищать клиентский узел, нужно установить и сконфигурировать выбранную программу.

Процедура

Если вы уже установили программу, начните с шага 2.

1. Выполните одно из следующих действий.
   - Чтобы установить программу в приложении или на клиентском узле, выполните инструкции.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows Совет: Можно также обновить существующие клиенты при помощи Центр операций. Инструкции смотрите в разделе Планирование обновлений клиента.
IBM Spectrum Protect for Databases	▪ Установка Data Protection for Oracle ▪ Установка Data Protection for SQL Server в ядре сервера Windows
IBM Spectrum Protect for Mail	▪ Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) ▪ Установка Data Protection for IBM Domino в системе Windows (V7.1.0) ▪ Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Программа	Ссылка на инструкции
IBM Spectrum Protect Snapshot	▪ Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux ▪ Установка и обновление IBM Spectrum Protect Snapshot для VMware ▪ Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Enterprise Resource Planning	▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 ▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- Чтобы установить программу на клиентском узле виртуальной машины, выполните инструкции для выбранного типа резервного копирования.

Тип резервного копирования	Ссылка на инструкции
Если вы собираетесь создавать полные резервные копии VMware виртуальных машин, установите и сконфигурируйте клиент резервного копирования и архивирования IBM Spectrum Protect.	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows
Если вы собираетесь установить постоянные полные резервные копии виртуальных машин, установите и сконфигурируйте IBM Spectrum Protect for Virtual Environments и клиент резервного копирования и архивирования на одном и том же клиентском узле или на разных клиентских узлах.	▪ Электронная документация по продукту IBM Spectrum Protect for Virtual Environments Совет: Программу для IBM Spectrum Protect for Virtual Environments и для клиента резервного копирования и архивирования можно получить в пакете установки IBM Spectrum Protect for Virtual Environments.

2. Чтобы разрешить клиенту соединяться с сервером, добавьте или обновите значения опций TCPSERVERADDRESS, TCPPORT и NODENAME в файле опций клиента. Используйте значения, записанные вами при регистрации клиента (раздел Регистрация клиентов).
   - Если клиенты установлены в операционной системе AIX, Linux или Mac OS X, добавьте значения в файл системных опций клиента, dsm.sys.
   - Если клиенты установлены в операционной системе Windows, добавьте значения в файл dsm.opt.

   По умолчанию, файлы опций находятся в каталоге установки.
3. Если вы установили клиент резервного копирования и архивирования в операционной системе Linux или Windows, то установите служба управления клиентами на клиенте. Следуйте инструкциям в разделе Установка службы управления клиентом.
4. Сконфигурируйте клиент для выполнения запланированных операций. Следуйте инструкциям в разделе Конфигурирование клиента для выполнения запланированных операций.
5. Необязательно: Сконфигурируйте связь через брандмауэр. Следуйте инструкциям в разделе Конфигурирование взаимодействий между клиентом и сервером через брандмауэр.
6. Запустите тестовое резервное копирование, чтобы проверить, защищены ли данные, как вы планировали. Например, для клиента резервного копирования и архивирования выполните следующие шаги:
   a. Выберите на странице Клиенты компонента Центр операций клиент, для которого вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
   b. Убедитесь, что резервное копирование выполнено успешно и что нет ни предупреждений, ни сообщений об ошибках.
7. Следите за результатами запланированных операций клиента в компоненте Центр операций.

Дальнейшие действия

Чтобы изменить набор объектов для резервного копирования, выполните инструкции в разделе Изменение объема резервного копирования клиента.

Конфигурирование клиента для выполнения запланированных операций

Вы должны сконфигурировать и запустить планировщик клиента на клиентском узле. Планировщик клиента обеспечивает взаимодействие между клиентом и сервером, чтобы могли выполняться запланированные операции. Например, запланированные операции обычно включают в себя резервное копирование файлов с клиента.

Об этой задаче

Предпочтительный метод заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций. Приемник клиента управляет планировщиком клиента, чтобы планировщик запускался, только когда это требуется:

- Когда наступило время запросить сервер о следующей запланированной операции
- Когда наступило время запустить следующую запланированную операцию

Используя приемник клиента, вы можете сократить число фоновых процессов на клиенте и помочь избежать проблем сохранения памяти.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, следуйте инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Если на вашем предприятии используется сторонний инструмент планирования в качестве стандартной практики, можно использовать этот инструмент планирования как альтернативу приемнику клиентов. Как правило, сторонние инструменты планирования запускают программы-клиенты напрямую, используя команды операционной системы. Чтобы сконфигурировать сторонний инструмент планирования, смотрите документацию по продукту.

Процедура

Чтобы сконфигурировать и запустить планировщик клиента с использованием приемника клиента, следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.
c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

   ```
   dsmc query sess
   ```

f. Запустите приемник клиента, введя в командной строке следующую команду:

   ```
   /usr/bin/dsmcad
   ```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте в файл запуска системы (обычно, /etc/inittab) следующую запись:

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Демон Client Acceptor
   ```

Linux

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.

c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

f. Запустите приемник клиента, войдя в систему от имени ID пользователя root и введя следующую команду:

```
service dsmcad start
```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте службу, введя в командной строке оболочки следующую команду:

```
# chkconfig --add dsmcad
```

MAC OS X

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Чтобы планировщик мог запускаться без участия оператора, щелкните по Авторизация, выберите Генерирование пароляи щелкните по Применить.
c. Чтобы указать, как осуществляется управление службами, щелкните по Веб-клиент, выберите Расписание, щелкните по Применить и выберите OK.
d. Чтобы сгенерированный пароль был сохранен, перезапустите клиент резервного копирования и архивирования.
e. Используйте для запуска приемника клиента приложение Инструменты IBM Spectrum Protect для администраторов.

Windows

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Утилиты > Мастер настройки > Помочь мне сконфигурировать Планировщик клиента. Щелкните по Далее.
b. Прочтите информации на странице мастера планировщика и нажмите Далее.
c. На странице Задача планировщика выберите Установить новый или дополнительный планировщик и нажмите Далее.
d. На странице Имя и расположение планировщика задайте имя для добавляемого планировщика клиента. Затем выберите Использовать Client Acceptor Daemon (CAD), чтобы управлять планировщиком, и нажмите Далее.
e. Введите имя, которое вы хотите присвоить этому приемнику клиента. Имя по умолчанию - Client Acceptor. Щелкните по Далее.
f. Выполните конфигурирование, выполняя шаги в мастере.
g. Обновите файл опций клиента, dsm.opt, и задайте для опции passwordaccess значение generate.
h. Чтобы сохранить пароль клиентского узла, введите в командной строке следующую команду:

```
dsmc query sess
```

Когда вам это предложат, введите пароль клиентского узла.
i. Запустите службу приемника клиента из панели Управление службами. Например, если вы использовали имя по умолчанию, запустите Служба Client Acceptor. Не запускайте службу планировщика, заданную вами на странице Имя и местонахождение планировщика. Служба планировщика автоматически запускается и останавливается службой приемника клиента по мере необходимости.

Конфигурирование взаимодействий между клиентом и сервером через брандмауэр

Если клиент должен связываться с сервером через брандмауэр, нужно включить связь между клиентом и сервером через брандмауэр.

Прежде чем начать

Если для регистрации клиентов вы использовали мастер добавления клиентов, найдите в файле опций клиента значения опций, полученные вами в ходе этого процесса. Для указания портов можно использовать значения.

Об этой задаче

Внимание: Не конфигурируйте брандмауэр, используя метод, который мог бы вызвать прекращение сеансов, используемых сервером или агентом хранения. Прекращение действительного сеанса может вызвать непредсказуемые последствия. Может показаться, что процессы и сеансы остановились из-за ошибок ввода-вывода. Чтобы помочь исключить сеансы из ограничений тайм-аута, сконфигурируйте известные порты для компонентов IBM Spectrum Protect. Убедитесь что для серверной опции KEEPALIVE осталось заданным значение по умолчанию YES. Это поможет вам убедиться, что связи клиент/сервер не прерывается. Инструкции относительно того, как задать опцию сервера KEEPALIVE смотрите в разделе KEEPALIVE.

Процедура

Откройте следующие порты, чтобы разрешить доступ через брандмауэр:

Порт TCP/IP для клиента резервного копирования и архивирования, административного клиента командной строки и планировщика клиента
: Задайте порт, используя опцию tcpport в файле опций клиента. Опция tcpport в файле опций клиента должна совпадать с опцией TCPPORT в файле опций сервера. Значение по умолчанию - 1500. Если вы решите использовать какое-либо значение, отличающееся от значения по умолчанию, задайте число в диапазоне 1024-32767.

Порт HTTP для включения взаимодействий между веб-клиентом и удаленными рабочими станциями
: Задайте порт для удаленной рабочей станции, задав опцию httpport в файле опций клиента удаленной рабочей станции. Значение по умолчанию - 1581.

Порты TCP/IP для удаленной рабочей станции
: Значение по умолчанию равно 0 (ноль); оно указывает, что два свободных номера портов случайным образом назначаются удаленной рабочей станции. Если вы не хотите, чтобы номера портов назначались произвольным образом, задайте значения, задав опцию webports в файле опций клиента удаленной рабочей станции.

Порт TCP/IP для сеансов администрирования
: Задайте порт, на котором сервер ожидает требований установления сеансов административного клиента. Значение опции клиента tcpadminport должно совпадать с опцией сервера TCPADMINPORT. Таким способом вы сможете защитить административные сеансы в частной сети.

Управление операциями клиентов

Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.

Об этой задаче

В некоторых случаях ошибки клиентов можно устранить, остановив и перезапустив приемник клиента. Если клиентские узлы или ID администратора окажутся заблокированы, вы сможете устранить проблему, разблокировав клиентский узел или ID администратора, а затем переустановив пароль.

Подробные инструкции по выявлению и устранению ошибок клиентов смотрите в разделе Устранение проблем клиентов.

- Оценка ошибок в журналах ошибок клиентов
  Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.
- Остановка и перезапуск приемника клиента
  Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.
- Изменение паролей
  Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

- Изменение объема резервного копирования клиента
  При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Оценка ошибок в журналах ошибок клиентов

Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.

Прежде чем начать

Чтобы устранить ошибки на клиенте резервного копирования и архивирования в операционной системе Linux или Windows, убедитесь, что у вас установлена и запущена служба служба управления клиентами. Инструкции по установке смотрите в разделе Установка службы управления клиентом. Инструкции по проверке установки смотрите в разделе Проверка того, правильно ли установлена служба управления клиентами.

Процедура

Чтобы диагностировать и устранить ошибки клиента, выполните одно из следующих действий:

- Если служба служба управления клиентами установлена на клиентском узле, выполните следующие шаги:
  1. На странице обзора в компоненте Центр операций щелкните по Клиенты и выберите клиент.
  2. Щелкните по Сведения.
  3. На странице Сводка клиента щелкните по вкладке Диагностика.
  4. Прочтите полученные сообщения журнала.
     Советы:
     - Чтобы показать или скрыть панель Журналы клиента, дважды щелкните по строке Журналы клиента.
     - Чтобы изменить размер панели Журналы клиента, щелкните по строке Журналы клиента и перетащите ее в нужное положение.

     Если на странице Диагностика показаны рекомендации, выберите рекомендацию. В панели Журналы клиента сообщения журнала клиента, с которыми связаны рекомендации, выделены.

  5. Используйте рекомендации, чтобы устранить проблемы, указанные в сообщениях об ошибках.
     Совет: Рекомендации предоставляются не для всех сообщений клиентов.
- Если служба служба управления клиентами не установлена на клиентском узле, смотрите журналы ошибок установленного клиента.

Остановка и перезапуск приемника клиента

Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

Об этой задаче

В некоторых случаях ошибки планирования клиентов можно устранить, остановив и перезапустив приемник клиента. Чтобы запланированные операции могли выполняться на клиенте, приемник клиента должен работать. Например, если вы измените IP-адрес или имя домене сервера, вы должны будете перезапустить приемник клиента.

Процедура

Следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- Чтобы остановить приемник клиента, выполните следующие действия:
  a. Определите ID процесса приемника клиента, введя в командной строке следующую команду:

     ```
     ps -ef | grep dsmcad
     ```

Ознакомьтесь с выводом. В приведенном ниже примере выходной информации 6764 - это ID процесса приемника клиента:

```
root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
```

b. Введите следующую команду в командной строке:

```
kill -9 PID
```

где *PID* задает ID процесса приемника клиента.

- Чтобы запустить приемник клиента, введите в командной строке следующую команду:

```
/usr/bin/dsmcad
```

Linux

- Чтобы остановить приемник клиента (но не перезапускать его), введите следующую команду:

```
# service dsmcad stop
```

- Чтобы остановить и перезапустить приемник клиента, введите следующие команды:

```
# service dsmcad restart
```

MAC OS X

Выберите Приложения > Утилиты > Терминал.

- Чтобы остановить приемник клиента, введите следующую команду:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Чтобы запустить приемник клиента, введите следующую команду:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Чтобы остановить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Остановить и OK.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Запуск и OK.

Ссылки, связанные с данной:
Устранение проблем расписаний клиентов

Изменение паролей

Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

Процедура

Чтобы устранить ошибки паролей, выполните одно из следующих действий:

- Если клиент резервного копирования и архивирования установлен на клиентском узле, а пароль был потерян или забыт, выполните следующие шаги:
  1. Сгенерируйте новый пароль, введя команду UPDATE NODE:

```
update node имя_узла
новый_пароль forcepwreset=yes
```

где *имя_узла* - это клиентский узел, а *новый_пароль* - это пароль, который вы назначаете.

2. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
   Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

- Если администратор окажется заблокирован из-за проблем, связанных с паролем, выполните следующие шаги:
  1. Чтобы обеспечить администратору доступ к серверу, введите команду UNLOCK ADMIN. Инструкции смотрите в разделе UNLOCK ADMIN (разблокирование администратора).
  2. Задайте новый пароль, используя команду UPDATE ADMIN:

     ```
     update admin имя_администратора
     новый_пароль
     forcepwreset=yes
     ```

     где *имя_администратора* - это имя администратора, а *новый_пароль* - это пароль, который вы назначаете.
- Если клиентский узел заблокирован, выполните следующие шаги:
  1. Определите, почему клиентский узел заблокирован и нужно ли его разблокировать. Например, если клиентский узел окажется списан, он удаляется из производственной среды. Обратить операцию списания нельзя, и клиентский узел останется заблокированным. Клиентский узел также может оказаться заблокированным, если данные клиента являются предметом юридического изучения.
  2. Если вам нужно разблокировать клиентский узел, используйте команду UNLOCK NODE. Инструкции смотрите в разделе UNLOCK NODE (Разблокировать клиентский узел).
  3. Сгенерируйте новый пароль, введя команду UPDATE NODE:

     ```
     update node имя_узла
     новый_пароль forcepwreset=yes
     ```

     где *имя_узла* задает имя узла, а *новый_пароль* - это пароль, который вы назначаете.
  4. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
     Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

Изменение объема резервного копирования клиента

При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Об этой задаче

Исключение ненужных объектов из операций резервного копирования позволяет лучше контролировать объем пространства хранения, необходимого для операций резервного копирования, а также расходы на хранение. В зависимости от вашего пакета лицензирования вам, возможно, также удастся ограничить расходы, связанные с лицензированием.

Процедура

То, как вы изменяете масштаб операций по резервному копированию, зависит от продукта, установленного на клиентском узле:

- Для клиента резервного копирования и архивирования можно создать список включения-исключения, чтобы включить файлы, группы файлов или каталоги в операции резервного копирования или исключить их из этих операций. Чтобы создать список включения-исключения, следуйте инструкциям в разделе Создание списка include-exclude.

  Чтобы обеспечить непротиворечивое использование списка включения-исключения для всех клиентов одного типа, можно создать на сервере набор опций клиента, содержащий необходимые опции. Затем вы назначаете набор опций клиента каждому из клиентов того же типа. Дополнительные сведения смотрите в разделе Управление операциями клиента через наборы опций клиентов.

- Для клиента резервного копирования и архивирования можно задать объекты в операции инкрементного резервного копирования, используя опцию domain. Следуйте инструкциям в разделе Domain, опция.
- В случае других продуктов, чтобы указать, какие объекты включаются в операции резервного копирования, а какие - исключаются из этих операций, следуйте инструкциям в документации по продукту.

Управление обновлениями клиентов

Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Прежде чем начать

1. Прочтите требования к совместимости клиентов/серверов в разделе Техническое замечание 1053218. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены.
2. Узнайте о требованиях к системе для клиента в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
3. Если решение содержит агенты хранения или библиотечные клиенты, ознакомьтесь с информацией о совместимости агентов хранения и библиотечных клиентов с серверами, сконфигурированными в качестве менеджеров библиотек. Смотрите раздел Техническое замечание 1302789.

   Если вы собираетесь обновить менеджера библиотек и библиотечный клиент, сначала нужно обновить менеджера библиотек.

Процедура

Для обновления программного обеспечения выполните инструкции, перечисленные в следующей таблице.

Программа	**Ссылка на инструкции**
Клиент резервного копирования и архивирования IBM Spectrum Protect	• Планирование обновлений клиента
IBM Spectrum Protect Snapshot	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Databases	• Обновление Data Protection for SQL Server • Установка Data Protection for Oracle • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0) • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Установка и обновление Data Protection for VMware • Установка Data Protection for Microsoft Hyper-V

Списание клиентского узла

Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).

Об этой задаче

При запуске процесса списания сервер блокирует клиентский узел, чтобы помешать ему получить доступ к серверу. Файлы, принадлежащие клиентскому узлу, постепенно удаляются, и затем удаляется клиентский узел. Можно списать следующие типы клиентских узлов:

Клиентские узлы приложения
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Клиентские узлы компьютеров
: В число клиентских узлов компьютеров входят рабочие станции, серверы файлов NAS и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Простейший метод списания клиентского узла заключается в том, чтобы использовать Центр операций. Процесс списания выполняется в фоновом режиме. Если клиент сконфигурирован для репликации данных клиента, Центр операций, прежде чем списать клиент, автоматически удалит клиент из репликации на исходном и целевом серверах репликации. Совет: Либо можно списать клиентский узел, введя команду DECOMMISSION NODE или DECOMMISSION VM. Вы можете счесть целесообразным использовать этот метод в следующих случаях:

- Чтобы запланировать процесс списания на будущее или выполнить ряд команд, используя сценарий, задайте выполнение процесса списания в фоновом режиме.
- Чтобы производить мониторинг процесса списания с целью отладки, задайте выполнение процесса списания в фоновом режиме. Если вы запустите процесс в активном режиме, вам придется дождаться завершения процесса, прежде чем вы сможете перейти к другим задачам.

Процедура

Выполните одно из следующих действий.

- Чтобы списать клиент в фоновом режиме, используя Центр операций, выполните следующие действия:
  1. На странице Обзор для компонента Центр операций щелкните по Клиенты и выберите клиент.
  2. Выберите Еще > Списать.
- Чтобы списать клиентский узел, используя команду администрирования, выполните следующие действия:
  1. Определите, сконфигурирован ли клиентский узел для репликации узла, введя команду QUERY NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

     ```
     query node austin format=detailed
     ```

     Проверьте выходное поле Состояние репликации.
  2. Если клиентский узел сконфигурирован для репликации, удалите клиентский узел из репликации, введя команду REMOVE REPLNODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

     ```
     remove replnode austin
     ```

  3. Выполните одно из следующих действий.
     - Чтобы списать клиентские узлы приложений или системные клиентские узлы в фоновом режиме, введите команду DECOMMISSION NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

```
decommission node austin
```

- Чтобы списать клиентские узлы приложений или системные клиентские узлы в активном режиме, введите команду DECOMMISSION NODE и задайте параметр `wait=yes`. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

  ```
  decommission node austin wait=yes
  ```

- Чтобы списать виртуальную машину в фоновом режиме, введите команду DECOMMISSION VM. Например, если имя виртуальной машины - AUSTIN, файловое пространство - 7, а имя файлового пространства задано с помощью ID файлового пространства, введите следующую команду:

  ```
  decommission vm austin 7 nametype=fsid
  ```

  Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

  ```
  decommission vm "austin 2" 7 nametype=fsid
  ```

- Чтобы списать виртуальную машину в активном режиме, введите команду DECOMMISSION VM и задайте параметр `wait=yes`. Например, введите следующую команду:

  ```
  decommission vm austin 7 nametype=fsid wait=yes
  ```

  Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

  ```
  decommission vm "austin 2" 7 nametype=fsid wait=yes
  ```

Дальнейшие действия

Следите за сообщениями об ошибках, которые могут появиться в пользовательском интерфейсе или в выходной информации команды сразу после запуска процесса.

Можно проверить, списан ли клиентский узел:

1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты.
2. В таблице Клиенты проверьте состояние в столбце Под угрозой:
   - Состояние DECOMMISSIONED (Списан) указывает, что узел списан.
   - Нулевое значение указывает, что узел не списан.
   - Состояние PENDING (Отложено) указывает, что узел списывается или процесс списания завершился неудачно.

   Совет: Если вы хотите определить состояние отложенного процесса списания, введите следующую команду:

   ```
   query process
   ```

3. Ознакомьтесь с выводом команды:
   - Если указано состояние для процесса списания, процесс выполняется. Например:

     ```
     query process

      Номер       Описание процесса                 Состояние процесса
       Число
     --------     --------------------     -------------------------------------------
            3           DECOMMISSION NODE         Number of backup objects deactivated
                                                  for node NODE1: 8 objects deactivated.
     ```

   - Если для процесса списания никакого состояния не указано и вы не получили сообщения об ошибке, процесс не завершен. Процесс может быть не завершен, если файлы, связанные с узлом, еще не деактивированы. После деактивации файлов снова запустите процесс списания.
   - Если для процесса списания никакого состояния не указано и вы получили сообщения об ошибке, это означает, что процесс завершился неудачно. Еще раз запустите процесс списания.

Ссылки, связанные с данной:
DECOMMISSION NODE (Списать клиентский узел)
DECOMMISSION VM (Списать виртуальную машину)
QUERY NODE (Запросить информацию об узлах)
REMOVE REPLNODE (Удалить клиентский узел из репликации)

Деактивация данных для высвобождения пространства хранения

В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Об этой задаче

Некоторые клиенты приложений всегда сохраняют данные на сервере как активные резервные копии данных. Поскольку активные резервные копии данных не управляются политиками устаревания перечня, данные не удаляются автоматически, и серверное хранилище используется до бесконечности. Чтобы высвободить пространство хранения, используемое устаревшими данными, можно деактивировать данные.

Когда вы запускаете процесс деактивации, все активные резервные копии данных, сохраненные до указанной даты, станут неактивными. Данные будут удалены по мере истечения срока их хранения, и восстановить их будет нельзя. Функция деактивации применяется только к клиентам приложений, которые защищают базы данных Oracle.

Процедура

1. На странице обзора в компоненте Центр операций щелкните по Клиенты.
2. В таблице Клиенты выберите один или несколько клиентов и щелкните по Еще > Очистить.
   Метод командной строки: Деактивируйте данные, используя команду DEACTIVATE DATA.

Ссылки, связанные с данной:
DEACTIVATE DATA (деактивация данных для клиентского узла)

Управление хранилищем данных

Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.

- Аудит контейнера пула хранения
  Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе данных и в контейнере в пуле хранения.
- Управление емкостью перечня
  Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.
- Управление использованием памяти и процессора
  Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.
- Тонкая настройка запланированных операций
  Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Ссылки, связанные с данной:
Типы пулов хранения

Аудит контейнера пула хранения

Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе данных и в контейнере в пуле хранения.

Об этой задаче

Вы производите аудит пулов хранения контейнеров в следующих случаях:

- При вводе команды QUERY DAMAGED обнаруживается ошибка
- Сервер выводит на экран сообщения о поврежденных экстентах данных

- Ваше оборудование сообщает о проблеме, и появляются сообщения об ошибках, связанные с пулом хранения контейнера

Процедура

1. Чтобы произвести аудит пула хранения на основе контейнеров, введите команду AUDIT CONTAINER. Например, введите следующую команду, чтобы произвести аудит контейнера, 000000000000076c.dcf:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Прочтите выходные данные сообщения ANR4891I, чтобы получить информацию о всех поврежденных экстентах данных.

Дальнейшие действия

При обнаружении проблем с пулом хранения контейнера вы можете восстановить данные на основе вашей конфигурации. Содержимое в пуле хранения можно исправить, используя команду REPAIR STGPOOL.
Ограничение: Содержимое в пуле хранения можно исправить, только если вы защитили пул хранения с использованием команды PROTECT STGPOOL.
Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения каталогов-контейнеров или в облачно-контейнерном пуле хранения)

Управление емкостью перечня

Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

Прежде чем начать

У активного и архивного журналов есть следующие особенности:

- Максимальный размер активного журнала равен 512 ГБ. Более подробную информацию о размерах активного журнала для вашей системы смотрите в разделе Планирование массивов хранения.
- Размер архивного журнала ограничен размером файловой системы, в которой он установлен. Размер архивного журнала не поддерживается на заранее заданном уровне, как в случае активного журнала. Архивные файлы журналов автоматически удаляются, когда они становятся больше не нужны.

(Необязательно) Лучше всего создать архивный журнал отказоустойчивости, чтобы сохранять файлы архивного журнала при переполнении каталога архивных журналов.

Проверьте Центр операций, чтобы определить, какой компонент перечня переполняется. Прежде чем увеличивать размер одного из компонентов перечня, убедитесь, чтобы вы остановили сервер.

Процедура

- Чтобы увеличить размер базы данных, выполните следующие шаги:
  - Создайте один или несколько каталогов для базы данных на отдельных накопителях или в файловых системах.
  - Введите команду EXTEND DBSPACE, чтобы добавить каталог или каталоги к базе данных. Каталоги должны быть доступны для ID пользователя экземпляра менеджера базы данных. По умолчанию данные перераспределяются по всем каталогам базы данных и пространство высвобождается.
    Советы:
    - Время, необходимое для полного перераспределения данных и высвобождения пространства, изменяется в зависимости от размера вашей базы данных. Убедитесь, что это учтено при планировании.
    - Убедитесь, что размер указанных каталогов совпадает с размером существующих каталогов, чтобы обеспечить согласованную степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.

- Остановите и перезапустите сервер для полного использования новых каталогов.
- Если потребуется, исправьте базу данных. Реорганизация индекса и таблиц для базы данных сервера может помочь избежать неожиданных проблем, связанных с ростом базы данных и производительностью. Дополнительную информацию о реорганизации базы данных смотрите в Техническое замечание 1683633.

- Чтобы уменьшить размер базы данных для серверов V7.1 и новее, введите следующие команды DB2 из каталога экземпляра сервера:
  Ограничение: Команды могут увеличить число операций ввода-вывода и повлиять на производительность сервера. Чтобы свести к минимуму проблемы производительности, подождите выполнения одной команды перед вводом следующей команды. Команды DB2 можно вводить, когда сервер работает.

  ```
  db2 connect to tsmdb1
  db2 set schema tsmdb1
  db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
  ```

- Чтобы увеличить или уменьшить размер активного журнала, выполните следующие шаги:
  1. Убедитесь, что в каталоге активного журнала достаточно пространства для увеличения размера журнала. Если существует зеркальная копия журнала, там, где она находится, также должно быть достаточно места для увеличения размера журнала.
  2. Отключите сервер.
  3. Измените в файле dsmserv.opt значение опции ACTIVELOGSIZE, задав новый размер активного журнала (в мегабайтах).
     Размер файла активного журнала основан на значении опции ACTIVELOGSIZE. Рекомендации по требованиям к объему пространства приведены в следующей таблице:

     Табл. 1. Как оценить требования к пространству томов и файлов

Значение опции ACTIVELOGSize	**Зарезервируйте этот объем свободного пространства в каталоге активного журнала в дополнение к пространству ACTIVELOGSize.**
16 ГБ - 128 ГБ	5120 МБ
129 ГБ - 256 ГБ	10240 МБ
257 ГБ - 512 ГБ	20480 МБ

     Чтобы изменить размер активного журнала до максимального размера, равного 512 ГБ, введите следующую серверную опцию:

     ```
     activelogsize 524288
     ```

  4. Если вы собираетесь использовать новый каталог активного журнала, измените имя каталога, заданное серверной опцией ACTIVELOGDIRECTORY. Новый каталог должен быть пустым, и он должен быть доступен для ID пользователя менеджера базы данных.
  5. Перезапустите сервер.
- Произведите сжатие архивных журналов, чтобы уменьшить объем пространства, необходимого для хранения. Разрешите динамическое сжатие архивного журнала следующей командой:

  ```
  setopt archlogcompress yes
  ```

Ограничение: Будьте внимательны, если вы разрешаете опцию сервера ARCHLOGCOMPRESS на компьютерах с постоянным высоким использованием томов и высокими рабочими нагрузками. Разрешение этой опции в такой среде может привести к задержкам при архивировании файлов журнала из файловой системы активного журнала в файловую систему архивного журнала. Задержка может привести к тому, что в файловой системе активного журнала не хватит места. Обязательно выполняйте мониторинг пространства, доступного в файловой системе активного журнала, после разрешения сжатия архивного журнала. Если использование файловой системы каталога активного журнала приближается к предельному, то запретите опцию сервера ARCHLOGCOMPRESS. Чтобы немедленно запретить сжатие архивного журнала без остановки сервера, введите команду SETOPT.

Ссылки, связанные с данной:
ACTIVELOGSIZE, серверная опция
EXTEND DBSPACE (увеличение емкости базы данных)
SETOPT (Задать динамическое обновление серверной опции)

Управление использованием памяти и процессора

Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.

Прежде чем начать

- Убедитесь, что в вашей конфигурации используются необходимые аппаратные и программные средства. Дополнительные сведения смотрите в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
- Дополнительную информацию об управлении ресурсами (например, база данных и журнал восстановления) смотрите в разделе Планирование массивов хранения.
- Добавьте больше системной памяти, чтобы определить, повышается ли при этом производительность. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память.

Процедура

1. Высвобождайте память из кэша файловой системы, если это возможно.
2. Для управления системной памятью, используемой каждым сервером в системе, используйте опцию DBMEMPERCENT. Ограничьте процентную долю системной памяти, которая может использоваться менеджером базы данных каждого сервера. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.
3. Задайте для базы данных предельный объем данных пользователя и собственной памяти, чтобы не вырабатывать собственную память. Если собственная память будет исчерпана, это может приводить к ошибкам, снижению производительности ниже оптимальной и нестабильности.

Тонкая настройка запланированных операций

Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Процедура

1. Регулярно отслеживайте производительность системы, чтобы убедиться, что задачи по резервному копированию клиента и по обслуживанию сервера выполняются успешно. Следуйте инструкциям в разделе Мониторинг дискового решения с несколькими площадками.
2. Необязательно: Если информация мониторинга показывает, что рабочая нагрузка сервера повышается, смотрите информацию о планировании. Проверьте, является ли емкость системы достаточной, в следующих случаях:
    - Число клиентов увеличивается
    - Объем данных, резервное копирование которых производится, возрастает
    - Время, доступное для резервного копирования, изменяется
3. Определите, работает ли ваше решение на том уровне, который вы ожидаете. Проверьте расписания клиентов, чтобы выяснить, выполняются ли задачи в течение запланированного периода времени:
    a. Выберите клиента на странице Клиенты Центра операций.

b. Щелкните по Сведения.
c. На странице Сводка на клиенте проверьте операции Создана резервная копия и Реплицирован, чтобы выявить все риски.

Скорректируйте время и частоту операций резервного копирования клиента, если потребуется.

4. Запланируйте достаточно времени для следующих задач по обслуживанию, чтобы они успешно выполнялись в течение 24-часового периода:
   a. Защищайте пулы хранения.
   b. Реплицируйте данные узлов.
   c. Создайте резервную копию базы данных.
   d. Запускайте обработку устаревания, чтобы удалить резервные и архивные копии файлов из серверного хранилища.

   Совет: Запланируйте задачи по обслуживанию, чтобы они запускались в соответствующее время в правильной последовательности. Например, запланируйте задачи репликации после успешного завершения операций по резервному копированию клиента.

- Перемещение клиентов с одного сервера на другой
  Чтобы не допустить нехватки пространства на сервере или устранить проблемы рабочей нагрузки, вам может потребоваться переместить клиентские узлы с одного сервера на другой.

Понятия, связанные с данным:
Производительность
Задачи, связанные с данной:
Как задать расписания для операций по обслуживанию сервера
Дедупликация данных (V7.1.1)

Управление репликацией

Используйте репликацию для восстановления данных на площадке восстановления после аварии и для поддержания одного уровня файлов на серверах источника и назначения. Вы можете управлять репликацией на уровне узлов. Вы также можете защитить данные на уровне пула хранения.

- Совместимость репликации
  Прежде чем настраивать операции репликации IBM Spectrum Protect, вы должны убедиться, что исходный сервер репликации и сервер репликации назначения совместимы для репликации.
- Как включить репликацию узлов
  Вы можете включить репликацию узлов, чтобы защитить данные.
- Защита данных в пулах хранения каталогов-контейнеров
  Защитите данные в пулах хранения каталогов-контейнеров, чтобы сократить время репликации узла и включить исправление данных в пулах хранения каталогов-контейнеров.
- Изменение параметров репликации
  Измените параметры репликации в Центр операций. Измените такие параметры, как число сеансов репликации, правила репликации, данные, которые вы хотите реплицировать, расписание репликации и рабочую нагрузку репликации.
- Как задать разные политики сохранения для исходного сервера и целевого сервера
  Вы можете задать политики на сервере назначения репликации, которые будут управлять реплицированными данными узлов-клиентов не так, как на исходном сервере. Например, можно обслуживать разное число версий файлов на исходном сервере и на сервере назначения.

Совместимость репликации

Прежде чем настраивать операции репликации IBM Spectrum Protect, вы должны убедиться, что исходный сервер репликации и сервер репликации назначения совместимы для репликации.

Табл. 1. Совместимость репликации для разных версий серверов

Версия сервера репликации источника	**Совместимые версии для сервера репликации назначения**
V7.1	Версия 7.1 или более поздняя
Версия 7.1.1	Версия 7.1 или более поздняя
V7.1.3	V7.1.3 или новее

Версия сервера репликации источника	Совместимые версии для сервера репликации назначения
V7.1.4	V7.1.3 или новее
V7.1.5	V7.1.3 или новее
V7.1.6	V7.1.3 или новее
Версия 7.1.7	V7.1.3 или новее
V7.1.8	V7.1.3 или новее
V8.1	V7.1.3 или новее
V8.1.1	V7.1.3 или новее
V8.1.2	V7.1.3 или новее
V8.1.3	V7.1.3 или новее
V8.1.4	V7.1.3 или новее
V8.1.5	V7.1.3 или новее

Как включить репликацию узлов

Вы можете включить репликацию узлов, чтобы защитить данные.

Прежде чем начать

Убедитесь, что исходный сервер и сервер назначения совместимы для репликации.

Об этой задаче

Реплицируйте клиентский узел, чтобы реплицировать все данные клиента, включая метаданные. По умолчанию, когда вы впервые запускаете сервер, репликация узлов будет отключена.
Советы:

- Чтобы сократить время обработки репликации, защитите пул хранения до репликации клиентских узлов. При запуске репликации узла экстенты данных, которые уже были реплицированы за счет защиты пула хранения, будут пропущены.
- Для репликации требуются увеличенные объемы памяти достаточная полоса пропускания для выполнения обработки. Задайте такие размеры базы данных и ее журналов, чтобы транзакции могли выполняться.

Процедура

Чтобы включить репликацию узлов, выполните в компоненте Центр операций следующие шаги:

a. Щелкните на странице Серверы по Сведения.
b. На странице Сведения щелкните по Свойства.
c. В разделе Репликация выберите Включена в поле Исходящая репликация.
d. Щелкните по Сохранить.

Дальнейшие действия

Выполните следующие действия:

1. Чтобы узнать, успешно ли выполнена репликация, смотрите раздел Контрольный список ежедневного мониторинга.
2. Операционные системы LinuxЕсли сервер IBM Spectrum Protect реплицирует узлы на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Следуйте инструкциям в разделе Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде.

Ссылки, связанные с данной:
Совместимость репликации

Защита данных в пулах хранения каталогов-контейнеров

Защитите данные в пулах хранения каталогов-контейнеров, чтобы сократить время репликации узла и включить исправление данных в пулах хранения каталогов-контейнеров.

Прежде чем начать

Убедитесь, что на целевом сервере репликации существует хотя бы один пул хранения каталогов-контейнеров. Включив репликацию в компоненте Центр операций, можно запланировать защиту пула хранения. Чтобы сконфигурировать репликацию и включить защиту пула хранения, выполните следующие шаги:

1. В строке меню компонента Центр операций установите указатель мыши на Хранение и щелкните по Репликация.
2. На странице Репликация щелкните по Пара серверов.
3. Выполните шаги в мастере Добавить пару серверов.

Об этой задаче

При защите пулов хранения каталогов-контейнеров производится резервное копирование экстентов данных в другой пул хранения, и это позволяет повысить производительность при репликации узлов. При запуске репликации узла экстенты данных, резервное копирование которых уже было произведено за счет защиты пула хранения, будут пропущены, что сокращает время обработки репликации. Можно задать расписание защиты пулов хранения несколько раз в день, чтобы успевать за изменениями данных.

Защищая пул хранения, вы не используете ресурсы, которые реплицируют существующие данные и метаданные, что позволяет повысить производительность сервера. Если вы хотите защищать только пул хранения и создавать только его резервную копию, нужно использовать пулы хранения каталогов-контейнеров.

Альтернативная стратегия защиты: В качестве альтернативы использованию репликации можно защитить данные в пулах хранения каталогов-контейнеров, скопировав их в пулы хранения контейнеров-копий. Данные в пулах хранения контейнеров-копий хранятся на ленточных томах. Ленточные копии, хранящиеся автономно, дают дополнительную возможность защиты путем аварийного восстановления в реплицированной среде.

Процедура

1. Либо, чтобы включить защиту пула хранения, можно использовать команду PROTECT STGPOOL с исходного сервера, чтобы произвести резервное копирование экстентов данных в пуле хранения каталога-контейнера. Например, чтобы защитить пул хранения каталога-контейнера с именем POOL1, введите следующую команду:

   ```
   protect stgpool pool1
   ```

   В процессе операции по выполнению команды PROTECT STGPOOL исправляются поврежденные экстенты в пуле хранения назначения. Чтобы исправить экстенты, они должны уже быть отмечены на сервере назначения как поврежденные. Например, команда AUDIT CONTAINER может выявить повреждение в пуле хранения назначения до ввода команды PROTECT STGPOOL.
2. Необязательно: Если поврежденные экстенты были исправлены в пуле хранения назначения и вы защищаете несколько исходных пулов хранения в одном пуле хранения назначения, выполните описанные ниже шаги, чтобы обеспечить полное исправление:
   a. Введите команду PROTECT STGPOOL для всех исходных пулов хранения, чтобы максимально исправить повреждение.
   b. Снова введите команду PROTECT STGPOOL для всех исходных пулов хранения. Для второй операции используйте параметр FORCERECONCILE=YES. Этот шаг гарантирует, что все исправления из других исходных пулов будут правильно распознаны для всех исходных пулов хранения.

Результаты

Если пул хранения каталога-контейнера защищен, вы сможете исправить пул хранения в случае его повреждения, используя команду REPAIR STGPOOL.
Ограничение: Если вы реплицируете клиентские узлы, но не защищаете пул хранения каталога-контейнера, вы не сможете исправить пул хранения.

Дальнейшие действия

Выполните следующие действия:

1. Чтобы увидеть состояние рабочей нагрузки по репликации, выполните инструкции в разделе Контрольный список ежедневного мониторинга.
2.  Операционные системы LinuxЕсли сервер IBM Spectrum Protect реплицирует узлы на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Следуйте инструкциям в разделе Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде.

Ссылки, связанные с данной:
Исправление и восстановление данных в пулах хранения каталогов-контейнеров
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
PROTECT STGPOOL (Защитить данные пула хранения)
Информация, связанная с данной:
Часто задаваемые вопросы о пулах хранения каталогов-контейнеров
Часто задаваемые вопросы о пулах хранения облачных контейнеров

Изменение параметров репликации

Измените параметры репликации в Центр операций. Измените такие параметры, как число сеансов репликации, правила репликации, данные, которые вы хотите реплицировать, расписание репликации и рабочую нагрузку репликации.

Об этой задаче

Вам может потребоваться настроить параметры репликации в следующих сценариях:

- Изменения приоритетов данных
- Изменения правил репликации
- Необходимость сделать целевым сервером другой сервер
- Запланированные процессы, отрицательно влияющие на производительность сервера

Процедура

Используйте компонент Центр операций, чтобы изменить параметры репликации.

Задача	Процедура
Измените правило репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация выберите правило репликации, которое вы хотите применить: Правило архивирования по умолчанию, Правило резервного копирования по умолчанию или Правило управления пространством по умолчанию. d. Щелкните по Сохранить.
Укажите, в течение какого времени сохраняются записи репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация введите срок в днях, в течение которого должны храниться записи репликации, в поле Сохранять хронологию репликации. Либо выберите переключатель Не сохранять, если вам не нужны записи репликации. d. Щелкните по Сохранить.
Задайте целевой сервер репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация задайте целевой сервер. d. Щелкните по Сохранить.

Задача	Процедура
Отмените процесс репликации.	a. Щелкните на странице Серверы по Активные задачи. b. Выберите процесс или сеанс, который вы хотите отменить. c. Нажмите кнопку Отмена.

Как задать разные политики сохранения для исходного сервера и целевого сервера

Вы можете задать политики на сервере назначения репликации, которые будут управлять реплицированными данными узлов-клиентов не так, как на исходном сервере. Например, можно обслуживать разное число версий файлов на исходном сервере и на сервере назначения.

Процедура

1. На исходном сервере репликации проверьте конфигурацию репликации и убедитесь, что исходный сервер репликации может взаимодействовать с целевым сервером репликации; для этого введите команду VALIDATE REPLPOLICY. Например, проверьте конфигурацию, используя имя одного из реплицируемых клиентских узлов:

   ```
   validate replication node1 verifyconnection=yes
   ```

2. На исходном сервере репликации введите команду VALIDATE REPLPOLICY, чтобы проверить различия в политиках на серверах репликации источника и назначения. Например, чтобы увидеть разницу в политиках на исходном сервере и на сервере назначения, CVT_SRV2, введите на исходном сервере следующую команду:

   ```
   validate replpolicy cvt_srv2
   ```

3. Обновите политики на сервере назначения, если это потребуется.
   Совет: Можно использовать компонент Центр операций, чтобы изменить политики на сервере назначения. Следуйте инструкциям в разделе Изменение политик.
   Например, чтобы хранить неактивные версии файлов на сервере назначения в течение более короткого времени, чем на исходном сервере, уменьшите значение параметра Резервные копии в классах управления, применимых к реплицированным данным клиента.
4. Включите политики сервера репликации назначения, так чтобы он использовал свои политики для управления реплицированными данными клиентского узла; для этого введите на исходном сервере команду SET DISSIMILARPOLICIES. Например, чтобы включить политики на сервере репликации назначения CVT_SRV2, введите на исходном сервере следующую команду:

   ```
   set dissimilarpolicies cvt_srv2 on
   ```

   В следующий раз, когда запустится процесс репликации, политики на сервере репликации назначения будут использоваться для управления реплицированными данными клиентского узла.
   Совет: Если вы сконфигурируете репликацию, используя Центр операций, а политики на исходном сервере репликации и на сервере репликации назначения не совпадают, будет использоваться политика, заданная для исходного сервера репликации. Если вы включите политику на сервере репликации назначения, используя команду SET DISSIMILARPOLICIES, будет использоваться политика, заданная для сервера репликации назначения. Если на сервере репликации назначения нет политики, используемой узлом на исходном сервере репликации, используется политика STANDARD.

Ссылки, связанные с данной:
EXPORT POLICY (экспорт сведений политики)
SET DISSIMILARPOLICIES (включить политики на сервере репликации назначения, чтобы управлять реплицированными данными)
VALIDATE REPLICATION (Проверить репликацию для клиентского узла)
VALIDATE REPLPOLICY (Проверить политики на сервере репликации назначения)

Защита сервера

Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.

- Понятия, касающиеся защиты
  Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.
- Управление администраторами
  Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.
- Изменение требований к паролям
  Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.
- Защита IBM Spectrum Protect в системе
  Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Понятия, касающиеся защиты

Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.

Transport Layer Security

Можно использовать протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS), чтобы обеспечить защиту транспортного слоя для безопасной связи между серверами, клиентами и агентами хранения. Если вы пересылаете данные между сервером, клиентом и агентом хранения, используйте SSL или TLS для шифрования данных.

Совет: Любая документация IBM Spectrum Protect, обозначенная как "SSL" или "выбрать SSL", применима к TLS.

SSL предоставляется Global Security Kit (GSKit), установленным с сервером IBM Spectrum Protect и используемым сервером, клиентом и агентом хранения.

Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных DB2, который используется какими-либо серверами IBM Spectrum Protect.

Каждый сервер, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатором (certificate authority, CA). Вы можете использовать свои собственные сертификаты или можете приобрести сертификаты у сертификатора (CA). Любой сертификат нужно установить и добавить к базе данных ключей для сервера IBM Spectrum Protect, клиента или агента хранения. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL. Некоторые сертификаты сертификаторов предварительно устанавливаются в базах данных ключей по умолчанию.

SSL устанавливается независимо от сервера IBM Spectrum Protect, клиента и агента хранения.

Уровни полномочий

При использовании каждого сервера IBM Spectrum Protect существует ряд доступных уровней административных полномочий, определяющих задачи, которые может выполнить администратор.

После регистрации администратору нужно предоставить полномочия, назначив для него один или несколько уровней административных полномочий. Администратор с системными полномочиями может выполнить любую задачу с сервером и назначить уровни полномочий для других администраторов, воспользовавшись командой GRANT AUTHORITY. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Администратор может зарегистрировать другие ID администраторов, предоставить им уровни полномочий, переименовать или удалить их, а также блокировать или разблокировать их доступ к серверу.

Администратор может управлять доступом к определенным клиентским узлам для ID пользователей root и ID пользователей, не являющихся пользователями root. По умолчанию, ID пользователя, не являющегося пользователем root, не может производить резервное копирование данных на узле. Используйте команду UPDATE NODE, чтобы изменить параметры узла и включить резервное копирование.

Пароли

По умолчанию сервер автоматически использует аутентификацию с помощью пароля. Если аутентификация пароля включена (on), все пользователи при получении доступа к серверу должны указывать пароль.

Используйте Lightweight Directory Access Protocol (LDAP), чтобы применить более строгие требования к паролям. Дополнительную информацию смотрите в разделе Управление паролями и процедурами входа (V7.1.1).

Табл. 1. Характеристики аутентификации паролей

Характеристика	**Дополнительная информация**
Значение регистра символов	Без учета регистра.
Срок действия пароля по умолчанию	90 дней. Отсчет начинается с момента первой регистрации на сервере ID администратора или клиентского узла. Если в течение этого периода пароль не изменится, пароль нужно будет изменить, когда пользователь в следующий раз получит доступ к серверу.
Число попыток ввода неправильного пароля	Для всех клиентских узлов можно установить максимальное количество последовательных попыток неправильного ввода пароля. После превышения данного значения сервер блокирует такой узел.
Длина пароля по умолчанию	8 символов Администратор может задать минимальную длину. Начиная с версии 8.1.4, минимальная длина паролей сервера по умолчанию изменилась с 0 до 8 символов.

Защита сеанса

Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами и назначается с использованием параметра SESSIONSECURITY.

Для параметра SESSIONSECURITY можно задать одно из следующих значений:

- Значение STRICT принудительно применяет наиболее высокий уровень защиты взаимодействий между серверами IBM Spectrum Protect, узлами и администраторами.
- Значение TRANSITIONAL указывает, что при обновлении программы IBM Spectrum Protect до V8.1.2 или новее используется существующий протокол связи. Это значение по умолчанию. Если задано SESSIONSECURITY=TRANSITIONAL, автоматически применяются более строгие параметры защиты при использовании более высоких версий протокола TLS и при обновлении программы до V8.1.2 или новее. После того как узел, администратор или сервер будет соответствовать требованиям для значения STRICT, защита сеанса автоматически обновится до значения STRICT, и объект больше не сможет проходить аутентификацию, исплользуя предыдущую версию клиента или более ранние протоколы TLS.
  Прим.: До обновления серверов обновлять клиенты резервного копирования и архивирования до V8.1.2 или новее не нужно. После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжат взаимодействовать с сервером, используя значение TRANSITIONAL, пока объект будет соответствовать требованиям для значения STRICT. Точно так же можно обновить клиенты резервного копирования и архивирования до V8.1.2 или новее до обновления серверов IBM Spectrum Protect, но обновлять серверы сначала не требуется. Связь между серверами и клиентами не прерывается.

Дополнительные сведения о значениях параметра SESSIONSECURITY смотрите в описаниях следующих команд.

Табл. 2. Команды, используемые, чтобы задать параметр SESSIONSECURITY

Объект	**Команда**
Клиентские узлы	• REGISTER NODE • UPDATE NODE
Администраторы	• REGISTER ADMIN • UPDATE ADMIN

Объект	Команда
Серверы	• DEFINE SERVER • UPDATE SERVER

Администраторы, прошедшие аутентификацию с использованием команды DSMADMC, команды DSMC или программы dsm, после аутентификации с использованием V8.1.2 или новее не смогут проходить аутентификацию с использованием более ранней версии. Чтобы устранить проблемы аутентификации администраторов, смотрите следующие советы:
Советы:

- Убедитесь, что все программы IBM Spectrum Protect, используемые учетной записью администратора для входа в систему, обновлены до V8.1.2 или новее. Если учетная запись администратора производит вход из нескольких систем, убедитесь, что сертификат сервера установлен в каждой системе.
- После того как администратор пройдет аутентификацию на сервере V8.1.2 или новее, используя клиент V8.1.2 или новее, администратор сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. Команду администратора можно вводить из любой системы.
- Если потребуется, создайте отдельную учетную запись администратора, чтобы использовать ее только при работе с клиентами и серверами, на которых работает V8.1.1 или более ранняя программа.

Принудительно примените наивысший уровень защиты взаимодействий с сервером IBM Spectrum Protect, сделав так, чтобы все узлы, администраторы и серверы использовали защиту сеанса STRICT. Можно воспользоваться командой SELECTЮ чтобы определить, какие серверы, узлы и администраторы используют защиту сеанса TRANSITIONAL, чтобы их обновить для использования защиты сеанса STRICT.

Задачи, связанные с данной:
Защита связи

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Процедура

Чтобы изменить параметры администратора, выполните описанные ниже шаги.

Задача	Процедура

Добавить администратора	Чтобы добавить администратора, ADMIN1, с системными полномочиями и задать пароль, выполните следующие шаги:
	a. Зарегистрируйте администратора и задайте Pa$#$twO в качестве пароля, введя следующую команду:
	`register admin admin1 Pa$#$twO`
	b. Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`

Задача	Процедура

Изменить административные полномочия	Измените уровень полномочий для администратора ADMIN1.
	• Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`
	• Аннулируйте системные полномочия администратора, введя следующую команду:
	`revoke authority admin1 classes=system`

Удалить администраторов	Аннулируйте для администратора ADMIN1 доступ к серверу IBM Spectrum Protect, введя следующую команду: `remove admin admin1`
Временно запретите доступ к серверу	Заблокируйте или разблокируйте администратора, введя команду LOCK ADMIN или UNLOCK ADMIN.

Изменение требований к паролям

Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.

Об этой задаче

Применяя аутентификацию на основе паролей и управляя ограничениями паролей, вы защищаете данные и серверы от потенциальных угроз безопасности.

Процедура

Чтобы изменить требования к паролям для серверов IBM Spectrum Protect, выполните описанные ниже задачи.

Табл. 1. Задачи по аутентификации для серверов IBM Spectrum Protect

Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число неудачных попыток в поле Предел неудачных попыток входа в систему. Значение по умолчанию при установке равно 0.
Задайте минимальную длину пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число символов в поле Минимальная длина пароля.
Задайте срок действия паролей.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте срок в днях в поле Общий срок действия паролей.

Задача	Процедура
Отключите аутентификацию на основе паролей.	По умолчанию сервер автоматически использует аутентификацию с помощью пароля. При аутентификации пароля все пользователи для получения доступа к серверу должны вводить пароль. Запретить аутентификацию пароля можно только для паролей, аутентификация которых выполняется на сервере (LOCAL). Отключая аутентификацию на основе паролей, вы делаете сервер доступным для угроз безопасности.

Задать метод аутентификации по умолчанию.	Введите команду SET DEFAULTAUTHENTICATION. Например, чтобы использовать сервер как метод аутентификации по умолчанию, введите следующую команду:
	
	`set defaultauthentication local`
	
	Чтобы обновить клиентский узел для аутентификации на сервере, включите `AUTHENTICATION=LOCAL` в команду UPDATE NODE:
	
	`update node authentication=local`

Понятия, связанные с данным:

Аутентификация пользователей IBM Spectrum Protect с использованием сервера LDAP

Управление паролями и процедурами входа (V7.1.1)

Защита IBM Spectrum Protect в системе

Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Процедура

Убедитесь, что неавторизованные пользователи не могут получить доступ к каталогам для базы данных сервера и экземпляра сервера. Оставьте для этих каталогов параметры доступа, которые вы сконфигурировали во время реализации.

- Ограничение доступа пользователей к серверу
  Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.
- Ограничение доступа путем ограничений портов
  Ограничьте доступ к серверу, применив ограничения портов.

Ограничение доступа пользователей к серверу

Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Процедура

1. После регистрации администратора с использованием команды REGISTER ADMIN используйте команду GRANT AUTHORITY, чтобы задать уровень полномочий администратора. Дополнительные сведения о том, как задавать и изменять полномочия, смотрите в разделе Управление администраторами.
2. Чтобы управлять полномочиями администратора на выполнение некоторых задач, используйте следующие две опции сервера:
   a. Вы можете задать уровень полномочий, который должен быть у администратора, чтобы он мог ввести команды QUERY и SELECT с опцией сервера QUERYAUTH. По умолчанию, не требуется никакого уровня полномочий. Данное требование можно изменить, указав один из уровней полномочий, включая системные.

b. Вы можете указать, что для команд, которые заставляют сервер записывать внешний файл за счет использования серверной опции REQSYSAUTHOUTFILE, требуются системные полномочия. По умолчанию, для выполнения таких команд необходимы системные полномочия.

3. Можно ограничить резервное копирование данных на клиентском узле, так чтобы его могли выполнять только ID пользователя root или авторизованные пользователи. Например, чтобы ограничить резервное копирование ID пользователя root, введите команду REGISTER NODE или UPDATE NODE и задайте параметр BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Ограничение доступа путем ограничений портов

Ограничьте доступ к серверу, применив ограничения портов.

Об этой задаче

В зависимости от ваших требований к защите вам может потребоваться ограничить доступ к отдельным серверам. Сервер IBM Spectrum Protect можно настроить на прием данных с четырех портов TCP/IP: двух - для обычных протоколов TCP/IP или протоколов Secure Sockets Layer (SSL)/Transport Layer Security (TLS), и двух, которые можно использовать только для протокола SSL/TLS.

Процедура

Чтобы указать нужные порты, можно задать опции сервера (смотрите раздел Табл. 1).

Табл. 1. Опции сервера и доступ к портам

Серверный параметр	Доступ к портам
TCPPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для отслеживания требований установления сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. Значение по умолчанию - 1500.
TCPADMINPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований установления сеансов, отличных от сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. По умолчанию используется значение, заданное опцией TCPPORT. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.
SSLTCPPORT	Задает адрес порта TCP/IP SSL для сервера. Этот порт принимает только сеансы с поддержкой SSL. Значения порта по умолчанию нет.
SSLTCPADMINPORT	Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает требования на установление сеансов SSL. Значения порта по умолчанию нет. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.

ограничения:
Следующие ограничения применяются при определении портов сервера только для SSL (SSLTCPPORT и SSLTCPADMINPORT):

- Если вы задаете порт сервера только SSL в параметре LLADDRESS в команде DEFINE SERVER или UPDATE SERVER, надо также задать параметр SSL=Yes.
- Если вы задаете порт сервера только SSL для опции TCPPORT клиента, то надо также задать YES для опции SSL клиента.

Ссылки, связанные с данной:
Планирование доступа через брандмауэр

Остановка и запуск сервера

Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите

сервер в производственном режиме.

Прежде чем начать

Чтобы остановить и запустить сервер IBM Spectrum Protect, требуются системные полномочия или полномочия оператора.

- Остановка сервера
  Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.
- Запуск сервера для задач обслуживания или реконфигурирования
  Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Остановка сервера

Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

Об этой задаче

При вводе команды HALT для остановки сервера происходят следующие действия:

- Все процессы и сеансы узлов клиентов будут отменены.
- Все текущие транзакции будут остановлены. (При перезапуске сервера будет произведен откат транзакций.)

Процедура

Чтобы подготовить систему и остановить сервер, выполните следующие шаги:

1. Запретите запуск новых сеансов клиентских узлов, введя команду DISABLE SESSIONS:

   ```
   disable sessions all
   ```

2. Определите, не выполняются ли какие-либо сеансы клиентских узлов или процессы, выполнив следующее:
   a. На странице Центра операций Обзор посмотрите в области Активность общее число процессов и сеансов, которые активны в настоящий момент. Если это число заметно отличается от значения, которое обычно показано во время повседневного управления хранением, то просмотрите другие индикаторы состояния в Центре операций, чтобы определить, ошибка ли это.
   b. Смотрите график в области Активность, чтобы сравнить объем сетевого трафика за следующие периоды:
      - Текущий период, то есть, самые последние 24 часа
      - Предыдущий период, то есть, за 24 часа до текущего периода

      Если на графике за предыдущий период показано ожидаемый объем трафика, существенные различия с графиком за текущий период могут указывать на проблему.
   c. Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения. Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, получите информацию о процессах при помощи команд администрирования. Введите команду QUERY PROCESS для запроса процессов и получения информации о сеансах при помощи команды QUERY SESSION.
3. Дождитесь завершения сеансов клиентских узлов или отмените их. Чтобы отменить процессы и сеансы, сделайте следующее:
   - Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   - Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   - Нажмите кнопку Отмена.
   - Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, отмените сеансы при помощи команд администрирования. Введите команду CANCEL SESSION, чтобы отменить сеанс и процессы при помощи команды CANCEL PROCESS.

Совет: Если процесс, который вы хотите отменить, ожидает монтирования ленточного тома, требование монтирования будет отменено. Например, если вы введете команду EXPORT, IMPORT или MOVE DATA, команда может инициировать процесс, для которого потребуется смонтировать ленточный том. Однако, если ленточный том монтируется автоматизированной библиотекой, операция отмены может не иметь силы, пока не завершится процесс монтирования. В зависимости от вашей системной среды на это может потребоваться несколько минут.

4. Остановите сервер с помощью команды HALT:

```
halt
```

Запуск сервера для задач обслуживания или реконфигурирования

Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

```
halt
```

2. Запустите сервер, используя метод, который вы используете в производственном режиме. Выполните инструкции для вашей операционной системы.
   - Операционные системы AIXЗапуск экземпляра сервера
   - Операционные системы LinuxЗапуск экземпляра сервера
   - Операционные системы WindowsЗапуск экземпляра сервера

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Планирование обновления сервера

Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.

Об этой задаче

Выполните следующие рекомендации:

- Предпочтительный метод - обновить сервер с использованием мастера установки. Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.
- Если доступны обновления и для серверного компонента, и для компонента Центр операций, выберите переключатели, указывающие, что нужно обновить оба компонента.

Процедура

1. Проверьте список пакетов исправлений и промежуточных исправлений. Смотрите раздел Техническое замечание 1239415.
2. Ознакомьтесь с усовершенствованиями продукта, описанными в файлах readme.
   Совет: Получив пакет установки со страницы сайт поддержки IBM Spectrum Protect, вы также сможете получить доступ к файлу readme.
3. Убедитесь что версия, до которой вы обновляете сервер, совместима с другими компонентами, например, с агентами хранения и клиентами библиотек. Смотрите раздел Техническое замечание 1302789.
4. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены. Смотрите раздел Техническое замечание 1053218.
5. Прочтите инструкции по обновлению. Обязательно создайте резервную копию базы данных сервера, информации о конфигурации устройств и файла хронологии томов.

Дальнейшие действия

Чтобы установить пакет исправлений или промежуточное исправление, следуйте инструкциям для вашей операционной системы:

- Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect

Информация, связанная с данной:
Процесс обновления и перенастройки - Часто задаваемые вопросы

Подготовка к отключению или обновлению системы

Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.

Об этой задаче

Убедитесь, что вы запланировали регулярные действия по управлению, защите и обслуживанию сервера.

Процедура

1. Отмените выполняющиеся процессы и сеансы, сделав следующее:
   a. Выберите в Центр операций на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   b. Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   c. Нажмите кнопку Отмена.
2. Остановите сервер с помощью команды HALT:

```
halt
```

Совет: Можно ввести команду halt из Центр операций, установив указатель мыши на значок Параметры и щелкнув по Построитель команд. Затем выберите сервер, введите `halt` и нажмите на клавишу ввода (Enter).

Реализация плана аварийного восстановления

Примените стратегию аварийного восстановления, чтобы восстановить приложения, если произойдет авария, и обеспечить высокую доступность сервера.

Об этой задаче

Определите требования к восстановлению после аварии, выявив бизнес-приоритеты для восстановления клиентского узла, системы, которые вы используете для восстановления данных, и то, есть ли у клиентских узлов соединение с сервером восстановления. Используйте репликацию и защиту пулов хранения для защиты ваших данных. Также нужно определить, как часто производится защита пулов хранения на основе каталогов-контейнеров.

- Выполнение отработки восстановления
  Запланируйте отработку аварийного восстановления, чтобы подготовиться к аудиту, удостоверяющему возможность восстановления сервера IBM Spectrum Protect и гарантирующему, что можно восстановить данные и возобновить операции после перебоя с питанием. Отработка также поможет вам убедиться, что можно восстановить все данные и возобновить операции, прежде чем возникнет критическая ситуация.

Восстановление от потери данных или системных отключений электричества

Вы можете восстановить данные IBM Spectrum Protect, которые были утрачены, когда произошла авария или системный перебой в питании. Можно восстановить пулы хранения каталогов-контейнеров, данные клиентов и базы данных.

Прежде чем начать

Спланируйте рабочую нагрузку клиента и сервера, чтобы обеспечить наивысшую производительность для вашей среды хранения. Введите команды PROTECT STGPOOL и REPLICATE NODE как часть вашего расписания. Защитите пул хранения до репликации клиентского узла. При запуске репликации узла экстенты данных, которые уже были реплицированы за счет защиты пула хранения, будут пропущены, что сокращает время обработки репликации.

Процедура

Используйте методы восстановления в зависимости от компоненте, который нужно восстановить.

Компонент, который нужно восстановить	**Процедура**	**Дополнительная информация**

Компонент, который нужно восстановить	**Процедура**	**Дополнительная информация**
Пул хранения каталога-контейнера	Чтобы восстановить пулы хранения каталогов-контейнеров, сделайте следующее: a. Просканируйте поврежденные экстенты данных в пуле хранения каталогов-контейнеров, используя команду AUDIT CONTAINER и задав параметр ACTION=SCANALL. b. Исправьте поврежденные экстенты данных в пуле хранения каталогов-контейнеров, используя команду REPAIR STGPOOL. Ограничение: Пул хранения можно исправить, только если пул хранения защищен. c. Удалите поврежденные экстенты данных, используя команду AUDIT CONTAINER и указав параметр ACTION=REMOVEDAMAGED.	Исправление пулов хранения данных

Компонент, который нужно восстановить	Процедура	Дополнительная информация
Клиентские данные	Требования: • Исходный сервер репликации, сервер репликации назначения и клиент должны быть на уровне версии 7.1 или новее. Если версия любого из серверов более старая, автоматическая передача управления отключается и вам придется положиться на передачу управления после сбоя вручную. Вручную сконфигурируйте клиент для автоматической передачи управления при отказе на целевой сервер для восстановления данных. Если вы включили автоматическую передачу управления для клиента, вы сможете восстановить данные, используя функцию автоматической передачи управления. Вы можете проверить, есть ли опция usereplicationfailover в файле опций клиента и задано ли для нее значение `yes`. Если исходный сервер недоступен из-за перебоя в питании, восстанавливайте данные с целевого сервера, используя автоматическую передачу управления. Совет: • Используйте команду SET FAILOVERHLADDRESS, чтобы задать IP-адрес для сервера репликации в случае передачи управления при сбое, если этот адрес отличается от IP-адреса, заданного для процесса репликации.	• Восстановление поврежденных данных от реплицированной копии • SET FAILOVERHLADDRESS (Задать высокоуровневый адрес переключения после отказа)

Компонент, который нужно восстановить	Процедура	Дополнительная информация
Database	Требования: • Чтобы восстановить базу данных после аварийной ситуации, у вас должна быть копия текущего файла конфигурации устройств. Заново создать файл конфигурации устройств нельзя. • Убедитесь, что у вас есть резервная версия базы данных. Восстановите базу данных IBM Spectrum Protect до наиболее актуального состояния или до определенной точки во времени, используя утилиту сервера DSMSERV RESTORE DB.	DSMSERV RESTORE DB (восстановление базы данных)

- Восстановление базы данных
  Возможно, вам придется восстанавливать базу данных IBM Spectrum Protect после аварии. Вы можете восстановить базу данных до наиболее актуального состояния или на указанный момент времени. Для восстановления базы данных у вас должны быть тома с полной или инкрементной копией базы данных или с моментальным снимком резервной копии базы данных.
- Восстановление поврежденных данных от реплицированной копии
  Если исходный сервер репликации недоступен, вы сможете восстановить поврежденные данные из реплицированной копии, которая хранится на целевом сервере репликации.
- Исправление пулов хранения данных
  Если произойдет авария или отключение питания системы, вы сможете восстановить дедуплицированные экстенты данных в пуле хранения каталогов-контейнеров.

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
DSMSERV RESTORE DB (восстановление базы данных)

Восстановление базы данных

Возможно, вам придется восстанавливать базу данных IBM Spectrum Protect после аварии. Вы можете восстановить базу данных до наиболее актуального состояния или на указанный момент времени. Для восстановления базы данных у вас должны быть тома с полной или инкрементной копией базы данных или с моментальным снимком резервной копии базы данных.

Прежде чем начать

Если каталоги базы данных и журнала восстановления потеряны, создайте их заново, прежде чем запускать серверную утилиту DSMSERV RESTORE DB. Например, введите следующие команды:Операционные системы AIX
Операционные системы Linux

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Операционные системы Windows

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Ограничения:

- Чтобы восстановить базу данных до ее последней версии, нужно найти каталог архивного журнала. Если вы не сможете найти каталог, вам удастся восстановить базу данных только на конкретный момент времени.
- Протокол Secure Sockets Layer (SSL) нельзя использовать для операции восстановления баз данных.
- Вы не сможете восстановить базу данных сервера, если уровень выпуска резервной копии базы данных отличается от уровня выпуска восстанавливаемого сервера. Например, если вы используете сервер версии 8.1 и попытаетесь восстановить базу данных версии 7.1, произойдет ошибка.

Об этой задаче

Операции восстановления на момент времени, как правило, используются в таких ситуациях, как аварийное восстановление, или для устранения последствий ошибок, которые могут вызвать противоречия в базе данных. Чтобы восстановить базу данных на момент, когда она была потеряна, восстановите ее до самой последней версии.

Процедура

Чтобы восстановить базу данных, используйте серверную утилиту DSMSERV RESTORE DB. Выберите один из следующих методов в зависимости от того, какую версию базы данных вы хотите восстановить:

- Восстановить базу данных до самой последней версии. Например, введите следующую команду:

  ```
  dsmserv restore db
  ```

- Восстановить базу данных на определенный момент времени. Например, чтобы восстановить базу данных на момент создания набора резервных копий от 19 апреля 2015 г., используйте следующую команду:

  ```
  dsmserv restore db todate=04/19/2015
  ```

Дальнейшие действия

Если бы вы восстановили базу данных, а на сервере существуют пулы хранения контейеров каталогов, то вы должны выявить противоречия между базой данных и файловой системой.

1. Если вы восстановили базу данных до точки во времени и не откладывали повторное использование пула хранения контейнеров каталогов, вы должны произвести аудит всех контейнеров. Чтобы произвести аудит контейнеров, введите следующую команду:

   ```
   audit container stgpool
   ```

2. Если сервер не может определить контейнеры в системе, то выполните следующие действия, чтобы открыть список контейнеров:
   a. Введите на клиенте администрирования следующую команду:

      ```
      select имя_контейнера from containers
      ```

   b. В файловой системе введите следующую команду для каталога пула хранения на исходном сервере:
   Совет: Каталог пула хранения будет показан в выходной информации команды:
    Операционные системы AIX  Операционные системы Linux

      ```
      [root@source]$ ls -lR
      ```

      Операционные системы Windows

      ```
      c:\source_stgpooldir>dir /s
      ```

   c. Сравните перечисленные контейнеры в файловой системе и на сервере.
   d. Введите команду AUDIT CONTAINER и укажите контейнер, которого нет в выходной информации сервера. Задайте параметр ACTION=REMOVEDAMAGED, чтобы удалить контейнер.
   e. Чтобы убедиться, что контейнеры удаляются из файловой системы, смотрите появившиеся сообщения.

Совет: Сервер IBM Spectrum Protect не распознает контейнеры, созданные после последнего резервного копирования базы данных. Удалите лишние файлы, существующие в вашей локальной файловой системе, по сравнению с файлами, существующими на сервере IBM Spectrum Protect.

Задачи, связанные с данной:
Репликация данных на клиентском узле после восстановления базы данных (V7.1.1)
Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
DSMSERV RESTORE DB (восстановление базы данных)

Восстановление поврежденных данных от реплицированной копии

Если исходный сервер репликации недоступен, вы сможете восстановить поврежденные данные из реплицированной копии, которая хранится на целевом сервере репликации.

Прежде чем начать

Имя сервера, указанное вами в сочетании с командой SET REPLSERVER, должно соответствовать имени существующего определения сервера. Оно также должно быть именем сервера, который следует использовать в качестве целевого сервера репликации. Если окажется, что имя сервера, заданное в этой команде, не соответствует имени существующего определения сервера, команда завершится неудачно.
Совет:

- Будьте осторожны при изменении или удалении целевого сервера репликации. Если вы измените целевой сервер репликации, реплицируемые данные клиентского узла будут отправлены на другой целевой сервер репликации. Если вы удалите целевой сервер репликации, данные клиентского узла не будут реплицироваться.

Процедура

1. Проверьте состояние репликации данных на целевом сервере. Состояние репликации указывает, была ли самое последняя резервная копия реплицирована на вторичный сервер.
2. Восстановите данные с целевого сервера репликации, задав исходный сервер репликации как целевой сервер репликации. Например, если вы хотите задать исходный сервер репликации как целевой сервер репликации, server1, введите следующую команду:

```
set replserver server1
```

Дальнейшие действия

При восстановлении базы данных IBM Spectrum Protect на исходном сервере репликации репликация автоматически выключается. Перед тем как повторно включить репликацию, определите, необходимы ли вам копии данных, хранящиеся на целевом сервере репликации.

Задачи, связанные с данной:
Репликация данных на клиентском узле после восстановления базы данных (V7.1.1)

Исправление пулов хранения данных

Если произойдет авария или отключение питания системы, вы сможете восстановить дедуплицированные экстенты данных в пуле хранения каталогов-контейнеров.

Прежде чем начать

Определите несоответствия между базой данных и пулом хранения каталогов-контейнеров, используя команду AUDIT CONTAINER. Выявив поврежденные экстенты данных в пуле хранения каталогов-контейнеров, вы сможете определить, какие экстенты данных следует исправить.

Прежде чем исправлять пул хранения, убедитесь, что пул хранения защищен с использованием команды PROTECT STGPOOL.

Процедура

1. Чтобы исправить пул хранения каталогов-контейнеров, используйте команду REPAIR STGPOOL. Например, чтобы исправить пул хранения STGPOOL1, введите следующую команду:

   ```
   repair stgpool stgpool1
   ```

2. Если поврежденный пул хранения задан как пул хранения назначения в команде PROTECT STGPOOL для одного или нескольких исходных пулов хранения, введите команду PROTECT STGPOOL для всех исходных пулов хранения.
3. Чтобы убедиться, что все поврежденные данные выявлены и исправления в других исходных пулах хранения, снова введите команду PROTECT STGPOOL для всех исходных пулов хранения и задайте параметр FORCERECONCILE=YES.
4. Чтобы удалить объекты, ссылающиеся на поврежденные данные, введите команду AUDIT CONTAINER и задайте параметр ACTION=REMOVEDAMAGED.
5. Если поврежденный пул хранения является пулом хранения назначения для репликации узла с одного или нескольких исходных серверов, снова введите команду REPLICATE NODE со всех исходных серверов.
6. При исправлении повреждения введите команду PROTECT STGPOOL, чтобы убедиться, что пул защищен, для другого пула хранения каталога-контейнера.

Дальнейшие действия

Убедитесь, что никаких поврежденных экстентов данных в выходной информации команды QUERY DAMAGED не показано.

Ссылки, связанные с данной:

Исправление и восстановление данных в пулах хранения каталогов-контейнеров

AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)

QUERY DAMAGED (Запросить поврежденные данные в пуле хранения каталогов-контейнеров или в облачно-контейнерном пуле хранения)

REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)

Ленточное решение

Это решение для защиты данных обеспечивает хранение на ленточном носителе, это гибкая и экономически доступная возможность долгосрочного хранения данных.

- Планирование решения защиты данных на основе ленты
  Спланируйте решение по защите данных, включающее в себя операции резервного копирования с диска на диск и на ленту и с диска на ленту, чтобы оптимизировать хранение.
- Реализация решения по защите данных на основе ленты
  Решение на основе ленты использует резервное копирование с диска на диск и на ленту и применяет промежуточное сохранение на диске для оптимизации хранения. Реализуя ленточное решение, можно включить долгосрочное хранение данных и добиться экономичной масштабируемости.
- Мониторинг ленточного решения
  После реализации решения IBM Spectrum Protect на основе ленты выполняйте мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.
- Управление операциями для ленточного решения
  Используйте эту информацию для управления операциями для реализации ленточного решения на сервере IBM Spectrum Protect.

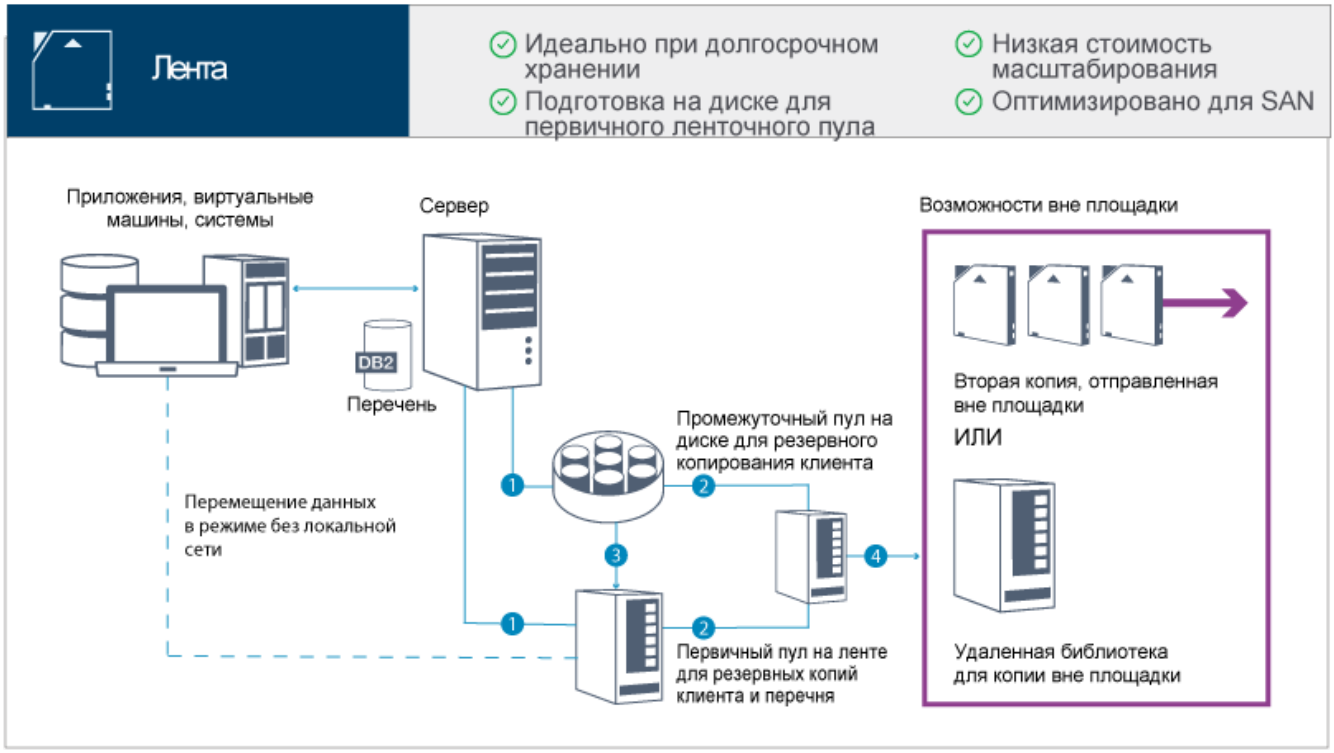
Планирование решения защиты данных на основе ленты

Спланируйте решение по защите данных, включающее в себя операции резервного копирования с диска на диск и на ленту и с диска на ленту, чтобы оптимизировать хранение.

Дорожная карта планирования

Запланируйте ленточное решение, ознакомившись со схемой архитектуры в разделе Рис. 1, а затем выполнив задачи в дорожной карте, которые приводятся после диаграммы.

Рис. 1. Ленточное решение



При такой конфигурации защиты данных сервер использует как дисковое, так и ленточное оборудование для хранения данных. Используется промежуточный пул хранения, когда данные клиентов первоначально сохраняются в дисковых пулах хранения, а потом переносятся в ленточные пулы хранения. Ленточные тома для восстановления после аварий можно хранить вне площадки. Опции вне площадки включают в себя физическое перемещение курьером второй копии вне площадки или электронное хранение копий вне площадки в удаленной библиотеке.

Совет: Описанное решение не включает в себя репликацию узлов. Однако, если вы хотите использовать репликацию узлов, чтобы создать резервную копию пула хранения с диска на диск, убедитесь, что операция репликации завершилась, прежде чем переносить данные с диска на ленту. Репликацию узлов также можно использовать для резервного копирования пула хранения на локальном ленточном устройстве в пул хранения копий на локальном ленточном устройстве.

Чтобы спланировать решение на основе магнитных лент, выполните следующие задачи:

1. Выполните требования к аппаратному и программному обеспечению.
2. Запишите значения конфигурации системы в рабочие листы планирования.
3. Спланируйте дисковое хранение.
4. Спланируйте ленточное хранение.
5. Спланируйте защиту.

Требования к планированию лент

Прежде чем реализовать ленточное решение, ознакомьтесь с общими рекомендациями относительно требований к системе. Определите, нужно ли производить резервное копирование данных на диск и/или на ленту.

Пропускная способность сети

У сети должна быть достаточная пропускная способность, соответствующая ожидаемой передаче данных между клиентом и сервером, и для выполнения операций восстановления с одной площадки на другую, если это требуется для аварийного восстановления. Используйте сеть хранения данных (Storage Area Network, SAN) для передачи данных между сервером, дисковыми устройствами и ленточными устройствами. Дополнительные сведения смотрите в разделе Требования к аппаратным средствам.

Перенос данных

Переносите все данные с диска на ленту ежедневно. Задайте для пулов хранения на основе дисков класс устройств FILE. Запланируйте перенос, чтобы управлять тем, когда будет происходить обработка. Чтобы предотвратить

автоматический перенос на основе порога переноса, задайте значение 100 для параметра HIGHMIG и значение 0 для параметра LOWMIG, когда будете вводить команду DEFINE STGPOOL. Вы должны оставить хотя бы 20% ленточных накопителей доступными для операций восстановления. Чтобы использовать до 80% доступных ленточных накопителей и повысить пропускную способность, задайте параметр MIGPROCESS.
Учтите следующую информацию, основанную на типе переносимых данных:

- Используйте ленту для резервного копирования данных с клиентов, на которых есть такие большие объекты, как базы данных.
  Совет: Обратитесь к производителю ленточных накопителей, чтобы получить рекомендации по размеру базы данных, подходящей для записи на ленту.
- Используйте диск для резервного копирования данных с клиентов, на которых есть объекты меньшего размера.
- Чтобы производить резервное копирование данных непосредственно на ленту, используйте перемещение данных в режиме без локальной сети. Дополнительные сведения смотрите в разделе Конфигурирование перемещения данных в режиме без сети;.
- Не производите резервное копирование виртуальных машин на ленту. Используйте отдельный пул хранения на основе дисков, который не перенсится в пул хранения на основе лент. Более подробную информацию о поддержке виртуальных машин смотрите в разделе technote 1239546.

Емкость пула хранения
: У вас должна быть достаточная емкость пула хранения, чтобы можно было в течение 2 дней производить резервное копирование клиента, и должно быть 20% для буфера. Возможно, вам придется запланировать полное резервное копирование через несколько дней, чтобы убедиться, что у вас достаточно пространства в пуле хранения.

Ленточные накопители
: Ознакомьтесь со спецификациями производителя и оцените емкость ленточного накопителя. Определите объем пространства, который потребуется для выполнения операций резервного копирования и переноса. Зарезервируйте 20% ленточных накопителей для операций восстановления.

Ссылки, связанные с данной:
MIGRATE STGPOOL (перенастройка пула хранения в следующий пул хранения)

Требования к системе для решения на основе ленты

Требования к аппаратному и программному обеспечению представлены для решения по хранения на основе лент со скоростью поглощения данных, равной 14 ТБ в час.

Однакомьтесь с этой информацией, чтобы узнать о требованиях к аппаратному и программному обеспечению для вашей среды хранения. Возможно, вам придется внести корректировки в зависимости от размера системы.

- Требования к аппаратным средствам
  Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.
- Требования к программному обеспечению
  Документация по решению IBM Spectrum Protect на основе лент содержит задачи по установке и конфигурированию для операционных систем IBM® AIX, Linux и Microsoft Windows. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Требования к аппаратным средствам

Требования к аппаратному обеспечению решения IBM Spectrum Protect основаны на размере системы. Чтобы обеспечить оптимальную производительность среды, выберите компоненты, эквивалентные тем, которые здесь перечислены, либо лучшие компоненты.

Более подробную информацию о планировании дисковых накопителей смотрите в разделе Планирование дискового хранилища.

Более подробную информацию о планировании ленточных накопителей смотрите в разделе Планирование ленточного хранилища.

В следующей таблице приводятся минимальные требования к аппаратному обеспечению для сервера и хранения. Если вы используете локальные разделы (LPAR) или рабочие разделы (WPAR), скорректируйте требования к сети, чтобы учесть размер разделов. Цифры в таблице основаны на скорости поглощения данных, равной 14 ТБ в час.

Аппаратный компонент	**Требования к системе**
Процессор сервера	 Операционные системы AIX8 ядер процессора, 3,42 ГГц или быстрее. Например, используйте основанный на процессоре POWER8 сервер.  Операционные системы Linux  Операционные системы Windows16 ядер процессора, 2,0 ГГц или быстрее. Например, используйте процессор Intel Xeon.
Память сервера	64 ГБ ОП.
Сеть	Указанный ниже размер управляет примерно 14 ТБ данных в час: • Ethernet на 10 Гбит (минимум четыре порта) • Адаптер Fibre Channel на 8 Гбит (минимум четыре порта) Число портов зависит от процента ежедневного поглощения данных в дисковые пулы хранения по сравнению с ленточным хранилищем. Используйте отдельные адаптеры Fibre Channel для данных на лентах и дисках.

Хранение	Диск
	В зависимости от того, какой объем данных вы записываете на диск, укажите нужное вам число дисков.
	
	Убедитесь, что пропусная способность последовательного ввода-вывода сети области хранения (storage area network, SAN) совпадает с пропускной способностью ввода-вывода для сети в предыдущей строке.
	
	Например, если вам нужно создавать резервные копии 10 ТБ данных в течение четырехчасового окна, пропускная способность будет составлять примерно 700 МБ в секунду. В этом случае серверу потребуется фронтальная сеть (путь с клиента на сервер), поддерживающая минимальную пропускную способность, равную 700 МБ в секунду. Внутренняя SAN (путь с сервера на устройство хранения) также должна поддерживать минимальную пропускную способность, равную 700 МБ в секунду.
	
	Чтобы вычислить необходимую скорость диска, используйте следующие формулы:
	
	`(Общий объем ежедневного поглощения данных - объем ежедневного поглощения данных непосредственно на ленту) (Число часов для ежедневных операций резервного копирования клиента) = Мегабайты поглощения данных на диск в час`
	
	`(Мегабайты поглощения данных на диск в час) ÷ (3600 секунд в час) = Мегабайты поглощения данных в секунду, которые должна поддерживать дисковая технология`
	
	Лента
	Выберите ленточную технологию, которая лучше всего соответствует вашим бизнес-требованиям. Например, используйте ленточные накопители IBM Linear Tape-Open (LTO) или IBM TS1150. Убедитесь, что у вас достаточно точек монтирования для операций резервного копирования клиентов и переноса. Более подробную информацию о планировании ленточного хранилища смотрите в разделе Планирование ленточного хранилища. Список поддерживаемых ленточных устройств смотрите в разделе IBM® для IBM Spectrum Protect. Совет: Чтобы оптимизировать перемещение данных, используйте перемещение данных в режиме без локальной сети.

Аппаратный компонент	Требования к системе
Адаптеры ввода-вывода SAN	Разделите дисковый и ленточный ввод-вывод. Более подробную информацию о выборе адаптера смотрите в документации по аппаратным продуктам Brocade и по решениям хранения IBM Storwize. Диск Используйте хотя бы два адаптера. Лента Используйте хотя бы два адаптера.

Оценка необходимого объема пространства для Центра операций

Требования к аппаратным средствам для Центр операций включены в предыдущую таблицу за исключением пространства базы данных и архивного журнала (перечня), которые используются компонентом Центр операций для удерживания записей для управляемых клиентов.

Если вы не собираетесь устанавливать Центр операций на том же компьютере, что и сервер IBM Spectrum Protect, вы можете оценить требования к системе отдельно. Чтобы вычислить требования к системе для компонента Центр операций, смотрите описание калькулятора требований к системе в документе техническое замечание 1641684.

Управление компонентом Центр операций на сервере IBM Spectrum Protect - это рабочая нагрузка, требующая дополнительного пространства для операций базы данных как на хаб-сервере, так и на всех подчиненных серверах. Объем пространства на хаб-сервере для архивного журнала будет больше, если хаб-сервер осуществляет мониторинг одного или нескольких подчиненных серверов. Прочтите следующие рекомендации, которые позволяют оценить, какой объем пространства потребуется вашему серверу IBM Spectrum Protect.

Пространство базы данных для Центр операций
: Компонент Центр операций использует, примерно, 4,4 ГБ пространства базы данных на каждую 1000 клиентов, отслеживаемых на этом сервере. Это вычисление относится как к хаб-серверам, так и к подчиненным серверам в пределах конфигурации.
Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1000 клиентов. Эта конфигурация дает в итоге 5000 клиентов на четырех серверах. Каждому из подчиненных серверов требуется 4,4 ГБ пространства базы данных. Если подчиненные серверы относятся к IBM Spectrum Protect версии 8.1.2 или новее, хаб-серверу потребуется 8,8 ГБ пространства базы данных только для мониторинга своих 2000 клиентов:

```
(4,4 ГБ x 2) = 8,8 ГБ
```

Пространство базы данных для управляемых данных
: *Управляемые данные* - это объем защищенных данных, включая объем данных для всех сохраненных версий.

- Для типов клиентов, которые выполняют резервное копирование Всегда инкрементное для оценки общего объема управляемых данных можно использовать приведенную ниже формулу:

  ```
  Фронтальный объем + (Фронтальный объем * Скорость изменений * (Срок хранения - 1)
  ```

  Например, если вы производите резервное копирование 100 ТБ фронтальных данных, используете 30-дневный срок хранения и у вас 5% скорость изменений, вычислите общий объем управляемых данных, используя следующие значения:

  ```
  100 ТБ + (100 ТБ × 0,5 × (30-1)) = Всего 245 ТБ управляемых данныхз
  ```

- Для типов клиентов, которые ежедневно выполняют полное резервное копирование для оценки общего объема управляемых данных можно использовать приведенную ниже формулу:

  ```
  Фронтальное хранение × (1 + скорость изменений)
  ```

Например, если вы производите резервное копирование 10 ТБ фронтальных данных, используете 30-дневный срок хранения и у вас 3% скорость изменений, вычислите общий объем управляемых данных, используя следующие значения:

```
10 ТБ × 30 × (1 + 0,03) = 309 ТБ управляемых данных
```

Неструктурированные данные, средний размер объекта: 4 Мб

Структурированные данные, средний размер объекта: 128 Мб

Неструктурированные данные, число объектов =

```
(245 Тб × 1024 × 1024) / 4 Мб = 64225280
```

Структурированные данные, число объектов =

```
(309 Тб × 1024 × 1024) / 128 Мб = 2531328
```

Общее число объектов: 66756608

Затраты на управляемые данные (1 КБ на объект) =

```
(66756608 КВ) / (1024 × 1024) = 63,66 Гб
```

Запланируйте 20% дополнительного пространства, чтобы системы базы данных не использовались на 100% емкости:

```
Требования
к общему физическому пространству хранения базы данных =
(управляемое пространство данных + пространство центра операций) × (1.20)
```

В этом примере вы вычислите пространство, используя следующие значения:

```
(66,33 ГБ + 8,4 ГБ) × 1,20 = 76,41 Гб
```

Пространство архивного журнала

Центр операций использует, примерно, 18 ГБ пространства архивного журнала каждые 24 часа на каждом сервере для каждой 1000 клиентов на этом сервере. Кроме того, для каждой 1000 клиентов, мониторинг которых осуществляется на подчитенных серверах, на хаб-сервере используется дополнительное пространство архивного журнала. В случае подчиненных серверов версии 8.1.2 или новее этот добавленный объем представляет собой 1,2 ГБ пространства архивного журнала на хаб-сервере на 1000 клиентов, отслеживаемых каждые 24 часа.

Например, рассмотрим хаб-сервер с 2000 клиентов, который также управляет тремя подчиненными серверами, на каждом из которых есть 1000 клиентов. Эта конфигурация дает в итоге 5000 клиентов на четырех серверах. Пространство архивного журнала для хаб-сервера можно вычислить по следующей формуле:

```
((18 ГБ x 2) + (1,2 ГБ x 3)) = 39,6 ГБ пространства архивного журнала
```

Эти оценки основаны на интервале сбора данных о состоянии по умолчанию, равном 5 минутам. Если вы сократите интервал сбора данных с одного раза за 5 минут до одного раза за 3 минуты, требования к пространству возрастут. В следующих примерах показано примерное увеличение требований к пространству журнала при интервале сбора данных один раз в 3 минуты для конфигурации, в которой производится мониторинг подчиненных серверов V8.1.2 или новее:

- Хаб-сервер: В диапазоне от 39,6 ГБ до 66 ГБ
- Каждый подчиненный сервер: В диапазоне от 18 ГБ до 30 ГБ

Выделите пространство архивного журнала, чтобы вы смогли поддерживать Центр операций, не влияя на операции сервера.

Требования к программному обеспечению

Документация по решению IBM Spectrum Protect на основе лент содержит задачи по установке и конфигурированию для операционных систем IBM® AIX, Linux и Microsoft Windows. У вас должны быть выполнены минимальные требования к программам из перечисленных.

Информацию о требованиях к программам для драйверов устройств IBM lin_tape смотрите в разделе Руководство по установке и использованию IBM Tape Device Drivers.

Системы AIX

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	IBM AIX 7.1 Дополнительную информацию о требованиях к операционным системам смотрите в разделе AIX: инимальные требования к системе для систем AIX.
Утилита gunzip	Утилита gunzip должна быть доступна в вашей системе до установки или обновления сервера IBM Spectrum Protect. Убедитесь, что утилита gunzip установлена и ее путь задан в переменной среды PATH.
Тип файловой системы	Файловые системы JFS2 Системы AIX могут кэшировать большие объемы данных файловой системы; при этом может сокращаться объем памяти, необходимый серверу и процессам IBM DB2. Чтобы избежать подкачки при использовании сервера AIX, используйте для файловой системы JFS2 опцию монтирования rbrw. Для кэша файловой системы используется меньше памяти, и для IBM Spectrum Protect будет доступно больше памяти. Не используйте опции монтирования файловой системы с параллельным вводом-выводом (Concurrent I/O, CIO) и с прямым вводом-выводом (Direct I/O, DIO) для файловых систем, содержащих журналы базы данных IBM Spectrum Protect или тома пулов хранения. Использование этих опций может вызывать снижение производительности многих серверных операций. IBM Spectrum Protect и DB2 все равно могут использовать DIO там, где это выгодно, но для IBM Spectrum Protect не требуются опции монтирования, чтобы выборочно использовать преимущества этого метода.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Linux

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Red Hat Enterprise Linux 7 (x86_64)
Библиотеки	Библиотеки GNU C версии 2.3.3-98.38 или новее, устанавливаемые в системе IBM Spectrum Protect. Серверы Red Hat Enterprise Linux: • libaio • libstdc++.so.6 (требуются 32- и 64-разрядные пакеты) • numactl.x86_64
Тип файловой системы	Сформатируйте файловые системы, связанные с базами данных, используя ext3 или ext4. Для файловых систем, связанных с пулами, используйте XFS.
Другое программное обеспечение	Оболочка Korn (ksh)

Системы Windows

Тип ПО	Минимальные требования к программному обеспечению
Операционная система	Microsoft Windows Server 2012 R2 (64-разрадная система) или Windows Server 2016
Тип файловой системы	NTFS

Тип ПО	Минимальные требования к программному обеспечению
Другое программное обеспечение	Должны быть установлены и включены Windows 2012 R2 или Windows 2016 с платформой .NET Framework 3.5. Должны быть отключены следующие политики управления учетными записями пользователей: • Управление учетными записями пользователей: Режим Утверждать администраторов для встроенной учетной записи Администратор • Управление учетными записями пользователей: Запускать всех администраторов в режиме Утверждать администраторов

Рабочие листы планирования

Используйте рабочие таблицы планирования, чтобы записывать в них значения, которые вы используете при настройке системы с последующим конфигурированием сервера IBM Spectrum Protect. Используйте наилучшие практические значения по умолчанию, приведенные в рабочих таблицах.

Каждая рабочая таблица поможет вам подготовиться к разным стадиям конфигурирования системы за счет использования наилучших практических значений:

Предварительное конфигурирование серверной системы
: Используйте рабочие таблицы предварительного конфигурирования для планирования файловых систем и каталогов, которые вы создадите, когда сконфигурируете файловые системы для IBM Spectrum Protect во время настройки системы. Все каталоги, созданные вами для сервера, должны быть пустыми.

Конфигурация сервера
: Воспользуйтесь рабочими таблицами по конфигурированию, когда будете конфигурировать сервер. Для большинства элементов предлагаются значения по умолчанию, кроме случаев, когда это отмечено.

Табл. 1. Рабочая таблица для предварительного конфигурирования серверной системы

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Адрес порта TCP/IP для взаимодействия с сервером	1500		Неприменимо.	Убедитесь, что этот порт доступен, когда будете устанавливать и конфигурировать операционную систему. Номер порта может быть числом в диапазоне от 1024 до 32767.
Каталог для экземпляра сервера	Операционные системы AIX Операционные системы Linux /home/tsminst1/tsminst1 Операционные системы Windows C:\tsminst1		Операционные системы AIX 50 ГБ. Операционные системы Linux Операционные системы Windows 25 ГБ.	Если вы измените значение каталога экземпляра сервера по сравнению со значением по умолчанию, измените также значение владельца экземпляра DB2 в Табл. 2.

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Каталог для установки сервера	 AIX  Linux /  Windows C:		 Доступное пространство, необходимое для каталога: 5 ГБ.  Linux  Минимальное пространство, необходимое для каталога: 30 ГБ	
Каталог для установки сервера	/usr		 Доступное пространство, необходимое для каталога: 5 ГБ.	
Каталог для установки сервера			 Доступное пространство, необходимое для каталога: 5 ГБ.	
Каталог для установки сервера	 /tmp		 Доступное пространство, необходимое для каталога: 5 ГБ.	
Каталог для установки сервера			 Доступное пространство, необходимое для каталога: 10 ГБ.	
Каталог для активного журнала	  /tsminst1/TSMalog  Windows C:\tsminst1\TSMalog		128 ГБ.	Если вы создаете активный журнал при первоначальном конфигурировании сервера, задайте размер, равный 128 ГБ.
Каталог для архивного журнала	  /tsminst1/TSMarchlog  Windows C:\tsminst1\TSMarchlog		3 ТБ.	

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Дополнительная информация
Каталоги для базы данных	Операционные системы AIX Операционные системы Linux /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 Операционные системы Windows C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03		Инструкции по вычислению требований пространства смотрите в разделе Требования к аппаратным средствам.	Создайте четыре файловых системы для базы данных.
Каталоги для хранения	Операционные системы AIX Операционные системы Linux /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ... Операционные системы Windows C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Определите минимальную общую емкость для всех каталогов, используя следующее вычисление: `Процент обработанных данных, ежедневно записываемых на диск + 20% = Минимальная общая емкость`	Предпочтительный метод - задать хотя бы один каталог для каждого ленточного устройства.

Табл. 2. Рабочая таблица для конфигурирования IBM Spectrum Protect

Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Владелец экземпляра DB2	tsminst1		Если вы изменили значение по умолчанию для каталога экземпляра сервера в таблице Табл. 1, то измените также значение владельца экземпляра DB2.
Пароль владельца экземпляра DB2	Операционные системы AIX Операционные системы Linux passw0rd Операционные системы Windows pAssW0rd		Выберите в качестве пароля владельца экземпляра значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Первичная группа для владельца экземпляра DB2	Операционные системы AIX Операционные системы Linux tsmsrvrs		
Имя сервера	Значением по умолчанию для имени сервера является системное имя хоста.		

Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Пароль сервера	passw0rd		Выберите в качестве пароля сервера значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
ID администратора: ID пользователя для экземпляра сервера	admin		
Пароль ID администратора	passw0rd		Выберите в качестве пароля администратора значение, отличающееся от значения по умолчанию. Обязательно запишите это значение и храните его в надежном месте.
Плановое время начала	23:00		Время начала расписания по умолчанию соответствует началу фазы рабочей нагрузки клиента, которая преимущественно состоит из операций резервного копирования и архивирования клиента. Во время фазы рабочей нагрузки клиента ресурсы сервера поддерживают операции клиента. Обычно эти операции завершаются в течение окна ночного расписания. Расписания для операций по обслуживанию сервера заданы так, чтобы они начинались через 10 часов после начала окна резервного копирования клиента. В этом руководстве рекомендуемое время для запуска операций резервного копирования клиента - 23:00.

Табл. 3. Рабочий лист для ленточного конфигурации

Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация

Элемент	Значение по умолчанию	Собственное значение	Дополнительная информация
Файлы роботизированных устройств	Устройства IBM® с драйвером ленточных устройств IBM:  Операционные системы AIX /dev/smcX  Операционные системы Linux /dev/IBMchangerX  Операционные системы Windows ChangerX Устройства не IBM с драйвером устройств IBM Spectrum Protect:  Операционные системы AIX /dev/lbX  Операционные системы Linux /dev/tsmscsi/lbX  Операционные системы Windows lbA.B.C.D		Чтобы вручную задать файлы устройств библиотеки, используйте следующие команды: • DEFINE LIBRARY • DEFINE DRIVE • DEFINE PATH Для SCSI можно использовать команду PERFORM LIBACTION, чтобы задать все накопители и их пути для одной библиотеки за один шаг. Чтобы использовать эту команду для назначения всех накопителей и путей, нужно, чтобы поддерживалась и была включена опция SANDISCOVERY.
Ленточные накопители	Устройства IBM с драйвером ленточных устройств IBM:  Операционные системы AIX /dev/rmtX  Операционные системы Linux /dev/IBMtapeX  Операционные системы Windows TapeX Устройства не IBM с драйвером устройств IBM Spectrum Protect:  Операционные системы AIX /dev/mtX  Операционные системы Linux /dev/tsmscsi/mtX  Операционные системы Windows mtA.B.C.D		

Планирование дискового хранилища

Выберите наиболее эффективную технологию хранения для компонентов IBM Spectrum Protect, чтобы обеспечить эффективную работу сервера и высокую производительность операций.

У аппаратных устройств хранения разные характеристики емкости и производительности, что определяет то, как их можно эффективно использовать вместе с IBM Spectrum Protect. Общие рекомендации по выбору соответствующего

оборудования хранения и настройке вашего решения смотрите в указанных ниже источниках.

База данных, активный журнал и архивный журнал

- Используйте твердотельный диск (SSD) или быстрый диск на 15000 об/мин для базы данных и активного журнала IBM Spectrum Protect.
- При создании массивов для базы данных используйте RAID уровня 5.
- Используйте отдельные диски для хранения резервной копии базы данных и архивного журнала.

Пул хранения
Используйте RAID уровня 6 для массивов пулов хранения, чтобы добавить защиту от двойных сбоев диска при использовании крупных типов дисков.

- Планирование массивов хранения
Подготовьтесь к конфигурированию дискового хранения, спланировав массивы RAID и тома в соответствии с размером вашей системы IBM Spectrum Protect.

Планирование ленточного хранилища

Определите, какие ленточные устройства нужно использовать и как их сконфигурировать. Чтобы оптимизировать производительность системы, запланируйте использование быстрых ленточных устройств с высокой мощностью. Предоставьте достаточно ленточных накопителей, чтобы их число удовлетворяло вашим бизнес-требованиям.

- Поддерживаемые ленточные устройства и библиотеки
Сервер может использовать широкий диапазон ленточных устройств и библиотек. Выберите ленточные устройства и библиотеки, соответствующие вашим бизнес-требованиям.
- Поддерживаемые конфигурации ленточных устройств
Ознакомьтесь с информацией о локальных сетях (Local Area Network, LAN) и сетях областей хранения данных (storage area network, SAN). Чтобы оптимизировать перемещение данных, запланируйте конфигурирование перемещения данных в режиме без локальной сети. Кроме того, рассмотрите возможность совместного использования библиотек.
- Определения, необходимые для ленточных устройств хранения
Перед тем как сервер IBM Spectrum Protect сможет использовать ленточное устройство, оно должно быть сконфигурировано для операционной системы и для сервера. Как часть процесса планирования, решите, какие определения требуются для ваших накопителей на магнитной ленте.
- Планирование иерархии пулов хранения
Спланируйте иерархию пулов хранения, чтобы ежедневно производился перенос данных с диска на ленту. При переносе высвобождается пространство на дисковом устройстве, и данные перемещаются на ленту для долгосрочного хранения. Это позволит вам воспользоваться преимуществами масштабируемости, экономической эффективности и функций защиты ленточного хранилища.
- Хранение данных вне площадки
Чтобы упростить восстановление данных и как часть стратегии аварийного восстановления храните копии лент вне площадки.

Поддерживаемые ленточные устройства и библиотеки

Сервер может использовать широкий диапазон ленточных устройств и библиотек. Выберите ленточные устройства и библиотеки, соответствующие вашим бизнес-требованиям.

Список поддерживаемых устройств и допустимых форматов классов устройств смотрите на веб-сайте для вашей операционной системы:

- Операционные системы AIXОперационные системы WindowsПоддерживаемые устройства для AIX и Windows
- Операционные системы LinuxПоддерживаемые устройства для Linux

Дополнительные сведения об устройствах хранения и объектах хранения смотрите в разделе Типы устройств хранения.

Каждое устройство, определенное для IBM Spectrum Protect, связывается с одним *классом устройств*. Каждый класс устройств задает информацию о типе устройств и управлении носителями, такую как формат записи, оценка емкости и префиксы маркировки.

Тип устройства определяет устройство как элемент группы устройств со схожими параметрами носителей. Например, тип устройств LTO применим ко всем поколениям ленточных накопителей LTO.

Класс устройств для ленточного накопителя должен задавать также библиотеку. *Физическая библиотека* представляет собой набор из одного или нескольких накопителей со схожими требованиями к монтированию носителей. То есть, накопитель может монтироваться оператором или механизмом автоматического монтирования.

Определение объекта библиотеки задает тип библиотеки и другие характеристики, связанные с этим типом библиотеки.

В следующей таблице перечислены предпочтительные типы библиотек для ленточного решения IBM Spectrum Protect версии 8.1.5.

Табл. 1. Типы библиотек для ленточного решения IBM Spectrum Protect 8.1.5

Тип библиотеки	**Описание**	**Дополнительная информация**
SCSI	Библиотека SCSI управляется с помощью интерфейса SCSI, подключенного либо непосредственно к хосту сервера с помощью кабелей SCSI, либо через сеть хранения данных. Монтирование и размонтирование ленточных томов автоматически выполняется роботом или другим механизмом. Если вы создадите другие типы накопителей для библиотеки SCSI, вы создадите несколько логических библиотек, которые нельзя разбить между разными типами накопителей. Библиотека SCSI может содержать накопители смешанных технологий, включая LTO Ultrium и накопители цифровых линейных лент (digital linear tape, DLT). Например: • Библиотека Oracle StorageTek L700 • Ленточное устройство IBM® 3592	Конфигурирование библиотек для использования сервером Ограничения применяются, если вы смешаете разные поколения носителей и накопителей. Дополнительные сведения смотрите в разделе: • Использование носителей 3592 разных поколений в одной библиотеке • Использование разных поколений накопителей и устройств LTO в библиотеке
Совместная	Совместно используемые библиотеки - это логические библиотеки, представленные SCSI. Библиотека управляется сервером IBM Spectrum Protect, настроенным как менеджер библиотеки. Серверы IBM Spectrum Protect, на которых используется тип библиотек SHARED, являются клиентами библиотеки по отношению к серверу менеджера библиотеки. Совместно используемые библиотеки ссылаются на менеджер библиотеки.	

Поддерживаемые конфигурации ленточных устройств

Ознакомьтесь с информацией о локальных сетях (Local Area Network, LAN) и сетях областей хранения данных (storage area network, SAN). Чтобы оптимизировать перемещение данных, запланируйте конфигурирование перемещения данных в режиме без локальной сети. Кроме того, рассмотрите возможность совместного использования библиотек.

Выберите конфигурацию устройства, которая соответствует вашим бизнес-требованиям.

- Перемещение данных в режиме с сетью и в режиме без сети
  Вы можете перемещать данные между клиентами и устройствами хранения, подключенными к локальной сети (local area network, LAN) или к устройствам хранения, подключенными к сети хранения данных (storage area network, SAN); это называется перемещением данных без локальной сети.
- Совместное использование библиотек
  Вы можете оптимизировать эффективность вашего ленточного решения, сконфигурировав совместное использование библиотек. Совместное использование библиотек позволяет нескольким серверам IBM Spectrum Protect использовать одну и ту же ленточную библиотеку и накопители в сети хранения (SAN, storage area network), повышая производительность резервного копирования и восстановления и уровень использования ленточного оборудования.
- перемещение данных в режиме без сети (LAN-free data movement)
  IBM Spectrum Protect позволяет клиенту с помощью агента хранения выполнять резервное копирование и восстановление данных непосредственно в ленточную библиотеку в сети SAN. Этот тип перемещения данных также называют перемещением данных в режиме без локальной сети.

- Смешанные типы устройств в библиотеке
  IBM Spectrum Protect поддерживает использование разных типов устройств в одной автоматизированной библиотеке, если библиотека может распознавать различные носители для разных типов устройств. Чтобы упростить процесс конфигурирования, не планируйте комбинирование разных типов устройств в библиотеке. Если вам нужно скомбинировать типы устройств, ознакомьтесь с ограничениями.

Перемещение данных в режиме с сетью и в режиме без сети

Вы можете перемещать данные между клиентами и устройствами хранения, подключенными к локальной сети (local area network, LAN) или к устройствам хранения, подключенными к сети хранения данных (storage area network, SAN); это называется перемещением данных без локальной сети.

В обычной конфигурации LAN одна или несколько ленточных библиотек связаны с одним сервером IBM Spectrum Protect. Перемещение данных без локальной сети делает ширину полосы пропускания локальной сети доступной для других видов использования и снижает нагрузку на сервер IBM Spectrum Protect.

В конфигурации локальной сети клиентские данные, электронная почта, терминальные подключения, приложение и информация для управления устройствами должны обслуживаться одной и той же сетью. Информация для управления устройством и клиентские данные резервного копирования и восстановления передаются по локальной сети.

Сеть хранения данных (SAN) - это выделенная сеть хранения, которая может дать выигрыш в производительности системы.

Применяя IBM Spectrum Protect в SAN, вы используете преимущества следующих функций:

- Совместно использовать устройства хранения на нескольких серверах IBM Spectrum Protect.
  Ограничение: Устройство хранения с типом устройства GENERICTAPE не может совместно использоваться серверами.
- Переместить данные клиента IBM Spectrum Protect непосредственно на устройства хранения (перемещение в режиме без локальной сети), сконфигурировав агент хранения в системе клиента.

В SAN можно совместно использовать ленточные устройства и библиотеки, поддерживаемые сервером IBM Spectrum Protect, в том числе большинство ленточных устройств SCSI.

Когда серверы IBM Spectrum Protect совместно используют ленту SCSI, один сервер, *менеджер библиотек*, владеет устройством и управляет им. Агенты хранения, вместе с другими серверами IBM Spectrum Protect, совместно использующими эту библиотеку - это *клиенты библиотеки*. Клиент библиотеки запрашивает совместно используемые ресурсы библиотеки, например, накопители или носители, у менеджера библиотеки, но использует ресурсы независимо. Менеджер библиотеки координирует доступ к этим ресурсам. Серверы IBM Spectrum Protect, определенные как клиенты библиотек, используют связи сервер-сервер для обращения к менеджеру библиотек и для требований служб устройств. Данные перемещаются по сети SAN между каждым сервером и устройством хранения.
Требование: Если вы зададите сервер менеджера библиотеки, который используется совместно с сервером IBM Spectrum Protect, для опции SANDISCOVERY нужно задать значение ON. По умолчанию для этой опции задано значение OFF.
Серверы IBM Spectrum Protect при совместном использовании автоматизированной библиотеки задействуют следующие функции:

Разбиение перечня томов
: Перечень томов носителей в совместно используемой библиотеке разделяется между серверами. Том либо принадлежит отдельному серверу, либо находится в глобальном чистом пуле. Чистый пул не принадлежит ни одному серверу.

Последовательный доступ к накопителям
: К каждому ленточному накопителю одновременно может обращаться только один сервер. Доступ к накопителям сериализован. IBM Spectrum Protect управляет доступом к накопителям, так чтобы серверы не размонтировали тома других серверов и не записывали данные на накопители, где другие серверы могут смонтировать свои тома.

Последовательный доступ для монтирования
: Авточейнджер библиотеки одновременно выполняет только одну операцию монтирования или размонтирования. Для обеспечения этой сериализации все операции монтирования выполняются одним сервером (менеджером библиотек).

Совместное использование библиотек

Вы можете оптимизировать эффективность вашего ленточного решения, сконфигурировав совместное использование библиотек. Совместное использование библиотек позволяет нескольким серверам IBM Spectrum Protect использовать одну и ту же ленточную библиотеку и накопители в сети хранения (SAN, storage area network), повышая производительность резервного копирования и восстановления и уровень использования ленточного оборудования.

При совместном использовании библиотеки на серверах IBM Spectrum Protect один сервер, сконфигурированный как менеджер библиотеки, управляет такими операциями библиотеки, как монтирование и размонтирование. Кроме того, менеджер библиотеки управляет правами собственности на тома и перечнем библиотеки. Остальные серверы, сконфигурированные как клиенты библиотеки, используют связь сервер-сервер для связи с менеджером библиотеки и запроса на использование ресурсов.

Клиенты библиотеки должны иметь такой же уровень версии, как у сервера - менеджера библиотеки, или более ранний. Менеджер библиотеки не может поддерживать клиентов библиотеки с более новым уровнем версии. Более подробную информацию смотрите в разделе Совместимость агента хранения и библиотечного клиента с сервером IBM Spectrum Protect.

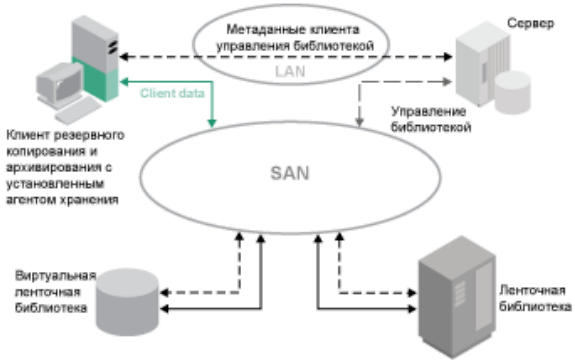
перемещение данных в режиме без сети (LAN-free data movement)

IBM Spectrum Protect позволяет клиенту с помощью агента хранения выполнять резервное копирование и восстановление данных непосредственно в ленточную библиотеку в сети SAN. Этот тип перемещения данных также называют перемещением данных в режиме без локальной сети.

Ограничение: Устройства хранения Centera не могут быть объектами назначения для операций в режиме без локальной сети.

На Рис. 1 показана конфигурация сети SAN, в которой клиент получает непосредственный доступ к ленте для чтения или записи данных.

Рис. 1. перемещение данных в режиме без сети (LAN-free data movement)



Перемещение данных в режиме без локальной сети требует установки агента хранения на клиентской системе. Сервер поддерживает базу данных и журнал восстановления и выступает в роли менеджера библиотеки для управления операциями устройства. Агент хранения на клиенте обрабатывает перенос данных на устройство в сети SAN. Такая реализация освобождает локальную сеть, которая в другом случае использовалась бы для перемещения клиентских данных.

Смешанные типы устройств в библиотеке

IBM Spectrum Protect поддерживает использование разных типов устройств в одной автоматизированной библиотеке, если библиотека может распознавать различные носители для разных типов устройств. Чтобы упростить процесс конфигурирования, не планируйте комбинирование разных типов устройств в библиотеке. Если вам нужно скомбинировать типы устройств, ознакомьтесь с ограничениями.

Библиотеки с этой возможностью - это модели со встроенными смешанными дисками или модели, поддерживающие добавление смешанных дисков. Информацию о конкретных моделях смотрите в документации производителя. Чтобы узнать о библиотеках, протестированных с IBM Spectrum Protect при использовании смешанных типов устройств, смотрите информацию для своей операционной системы:

- IBM Spectrum Protect: Поддерживаемые устройства для AIX, HP-UX, Solaris и Windows
- IBM Spectrum Protect: Поддерживаемые устройства для Linux

Например, в одной библиотеке, заданной для сервера IBM Spectrum Protect, у вас могут быть накопители LTO Ultrium и накопители IBM TS4500.

- Разные поколения носителей в библиотеке
  Сервер IBM Spectrum Protect позволяет использовать устройства разных типов в автоматизированной библиотеке, но использование устройств одного типа, но разных поколений, в общем случае не поддерживается. Новые накопители не могут записывать данные на носители более ранних форматов, а устаревшие накопители не могут считывать данные новых форматов. Исключением из этого правила являются накопители LTO Ultrium.
- Носители разных типов в пулах хранения
  Вы можете оптимизировать эффективность вашего ленточного решения, не смешивая форматы данных в пуле хранения. Вместо смешения форматов отобразите каждый уникальный формат данных в отдельный пул хранения, используя его собственный класс устройств. Это ограничение также относится к форматам LTO.

Разные поколения носителей в библиотеке

Сервер IBM Spectrum Protect позволяет использовать устройства разных типов в автоматизированной библиотеке, но использование устройств одного типа, но разных поколений, в общем случае не поддерживается. Новые накопители не могут записывать данные на носители более ранних форматов, а устаревшие накопители не могут считывать данные новых форматов. Исключением из этого правила являются накопители LTO Ultrium.

Если технология, используемая в новом накопителе, не позволяет записывать данные на носители, отформатированные с помощью устройств более раннего поколения. Во избежание проблем с операциями на сервере более ранние носители должны быть обозначены как предназначенные только для чтения. Кроме того, более старые накопители нужно удалить из библиотеки, или нужно удалить определения более старых накопителей с сервера. Например, сервер IBM Spectrum Protect не поддерживает использование накопителей Oracle StorageTek 9940 A с накопителями 9940B в сочетании с другими типами устройств в одной библиотеке.

В общем случае, IBM Spectrum Protect не поддерживает смешение поколений накопителей и носителей LTO Ultrium. Однако поддерживаются следующие комбинации:

- LTO Ultrium поколения 3 (LTO-3) с LTO Ultrium поколения 4 (LTO-4)
- LTO Ultrium поколения 4 (LTO-4) с LTO Ultrium поколения 5 (LTO-5)
- LTO Ultrium поколения 5 (LTO-5) с LTO Ultrium поколения 6 (LTO-6)
- LTO Ultrium поколения 6 (LTO-6) с LTO Ultrium поколения 7 (LTO-7)
- Носители LTO Ultrium поколения 7 (LTO-7) с носителем LTO Ultrium поколения 8 (LTO-8 и LTO-M8) в библиотеке с ленточными накопителями LTO-8 или библиотекой с ленточным накопителями LTO-8 и LTO-7

Сервер поддерживает эти сочетания, поскольку разные накопители могут считывать и записывать данные на различные носители. Если вы собираетесь обновить все накопители до поколения 4 (либо поколения 5, 6, 7 или 8), вы должны удалить все существующие определения накопителей LTO Ultrium и связанные с ними пути. После этого вы можете задать новые накопители и пути для накопителей поколения 4 (либо поколения 5, 6, 7 или 8).

Ограничения, применимые к смешению ленточных накопителей и носителей LTO Ultrium

- Накопители LTO-5 могут читать только носители LTO-3. Если в одной библиотеке одновременно используются накопители и носители LTO-3 с накопителями и носителями LTO-5, вы должны пометить носитель LTO-3 как доступный только для чтения. Нужно зарезервировать все чистые тома LTO-3.
- Накопители LTO-6 могут читать только носители LTO-4. Если в одной библиотеке одновременно используются накопители и носители LTO-4 с накопителями и носителями LTO-6, вы должны пометить носитель LTO-4 как доступный только для чтения. Нужно зарезервировать все чистые тома LTO-4.
- Накопители LTO-7 могут читать только носители LTO-5. Если в одной библиотеке одновременно используются накопители и носители LTO-5 с накопителями и носителями LTO-7, вы должны пометить носитель LTO-5 как доступный только для чтения. Нужно зарезервировать все чистые тома LTO-5.
- Накопители LTO-8 не способны читать носители LTO-6. Если вы смешиваете накопители и носители LTO-6 с накопителями и носителями LTO-8 в одной библиотеке, вы должны разбить библиотеку на две библиотеки. В одной библиотеке должны быть только накопители и носители LTO-8, а в другой - только накопители и носители LTO-6.

Ограничения, применимые к смешению поколений ленточных накопителей LTO Ultrium в библиотеке

Нужно использовать ленточные картриджи, относящиеся к более раннему поколению, чем ленточный накопитель. Ленточный накопитель более нового поколения может читать данные с ленточных картриджей более раннего поколения и может записывать на них данные. Например, если в библиотеке есть ленточные накопители LTO-7 и LTO-6, нужно использовать ленточные картриджи LTO-6. Как ленточные накопители LTO-7, так и ленточные накопители LTO-6 могут читать данные с ленточных картриджей LTO-6 и могут записывать на них данные.

Ограничения, применимые к смешению поколений ленточных картриджей LTO Ultrium в библиотеке

Следует использовать ленточный картридж, относящийся к тому же поколению, что и ленточный накопитель, или более ранний на одно поколение. Например, если в библиотеке есть ленточные накопители LTO-7, можно использовать ленточные картриджи LTO-7 или комбинацию ленточных картриджей LTO-7 и LTO-6. Если в этой библиотеке есть ленточные картриджи LTO-7, LTO-6 и LTO-5, нужно изменить режим доступа на READONLY для ленточных картриджей LTO-5.

Чтобы узнать о дополнительных замечаниях, связанных с использованием разных поколений LTO Ultrium, смотрите раздел Как задать классы устройств LTO.

При использовании IBM Spectrum Protect нельзя смешивать накопители поколений 3592, TS1130, TS1140, TS1150 и новее. Используйте одну из трех особых конфигураций. Дополнительные сведения смотрите в разделе Как задать классы устройств 3592.

Если в библиотеке будет выполняться шифрование томов, не используйте носители разных поколений в библиотеке.

Носители разных типов в пулах хранения

Вы можете оптимизировать эффективность вашего ленточного решения, не смешивая форматы данных в пуле хранения. Вместо смешения форматов отобразите каждый уникальный формат данных в отдельный пул хранения, используя его собственный класс устройств. Это ограничение также относится к форматам LTO.

Несколько пулов хранения и их классы устройств разных типов могут указывать на одну библиотеку, поддерживающую их, как описано в разделе Разные поколения носителей в библиотеке.

Можно выполнить переход на тип носителей нового поколения в пределах одного пула хранения, выполнив следующие шаги:

1. Замените в библиотеке все более старые накопители на накопители более нового поколения. Накопители должны комбинироваться.
2. Пометьте существующие тома с более старым форматом как тома только для чтения, если новый накопитель не может добавить эти ленты в старом формате. Если новый диск может записывать данные на существующие носители старого формата, это действие можно пропустить. Однако все равно необходимо выполнить шаг 1. Если это необходимо, чтобы оставить в одной и той же библиотеке разные поколения накопителей, которые совместимы по чтению, но несовместимы по записи, используйте для каждого из них отдельные пулы хранения.

Определения, необходимые для ленточных устройств хранения

Перед тем как сервер IBM Spectrum Protect сможет использовать ленточное устройство, оно должно быть сконфигурировано для операционной системы и для сервера. Как часть процесса планирования, решите, какие

определения требуются для ваших накопителей на магнитной ленте.

Совет: Команду PERFORM LIBACTION можно использовать для упрощения процесса, когда вы добавляете устройства в типы библиотек SCSI и VTL.

В Табл. 1 содержится сводка определений, необходимых для различных типов устройств.

Табл. 1. Определения, необходимые для устройств хранения

Устройство	Типы устройств	Необходимые определения			
		Библиотека	**Накопитель**	**Путь**	**Класс устройств**
Магнитный диск	DISK	—	—	—	Да [1]
	FILE [2]	—	—	—	Да
	Операционные системы AIX Операционные системы Windows CENTERA Операционные системы Linux CENTERA [3]	—	—	—	Да
Лента	• 3590 • 3592 • DLT • LTO • NAS • VOLSAFE Операционные системы AIX Операционные системы Windows GENERICTAPE ECARTRIDGE [4]	Да	Да	Да	Да
Сменный носитель (файловая система)	REMOVABLEFILE	Да	Да	Да	Да

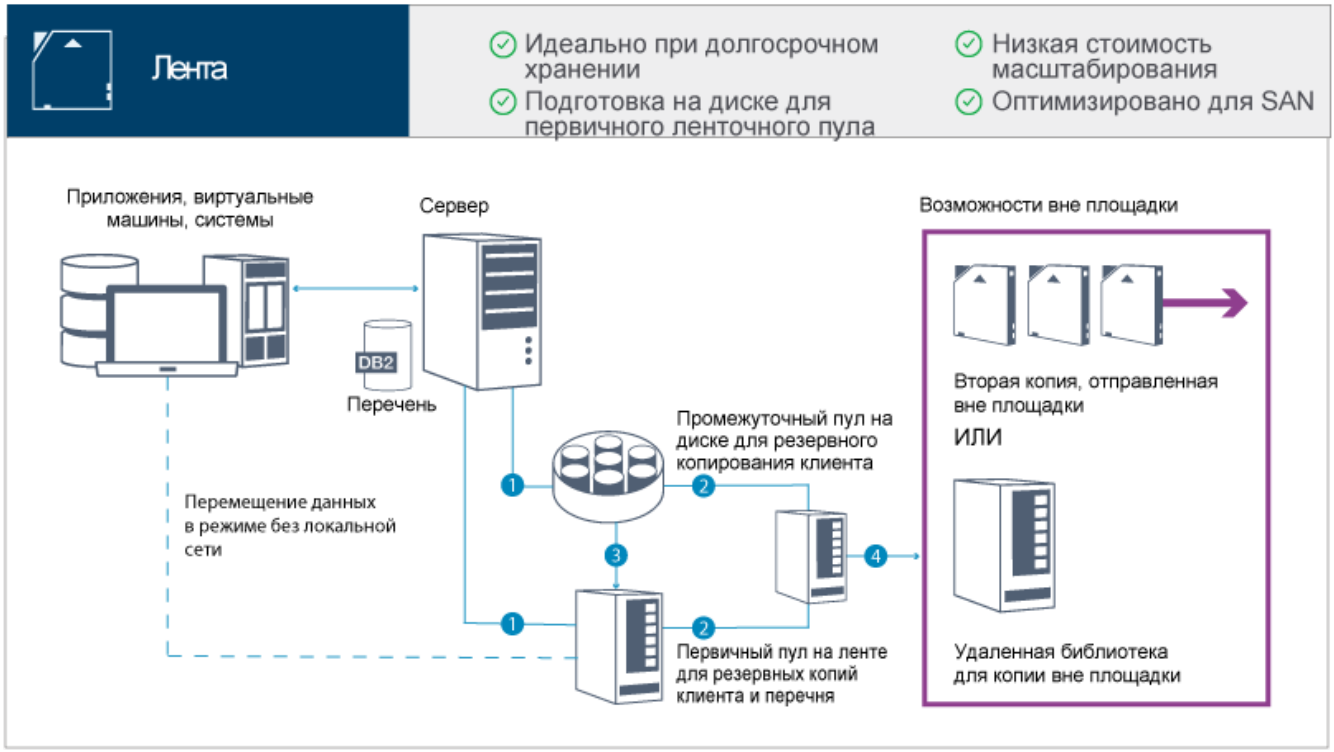
1. Класс устройств DISK присутствует при установке и не может быть изменен.
2. Библиотеки FILE, накопители и пути необходимы для совместного использования с агентами хранения.
3. Операционные системы LinuxТип устройств CENTERA доступен только для систем Linux x86_64.
4. Тип устройств ECARTRIDGE предназначен для накопителей с ленточными картриджами Oracle StorageTek, например, для накопителей 9840 и T10000.

Планирование иерархии пулов хранения

Спланируйте иерархию пулов хранения, чтобы ежедневно производился перенос данных с диска на ленту. При переносе высвобождается пространство на дисковом устройстве, и данные перемещаются на ленту для долгосрочного хранения. Это позволит вам воспользоваться преимуществами масштабируемости, экономической эффективности и функций защиты ленточного хранилища.

Прежде чем начать

Иерархия пулов хранения помогает управлять потоком данных. Чтобы понять этот поток данных, ознакомьтесь с Рис. 1.
Рис. 1. Ленточное решение



Следующие шаги соответствуют номерам на рисунке:

1. Сервер получает данные с клиентов (из приложений, с виртуальных машин или из систем) и сохраняет данные в первичных пулах хранения. В зависимости от типа клиента данные хранятся в первичном пуле хранения на диске или на ленте.
2. Производится резервное копирование данных на диске и на ленте в пул хранения копий на ленте.
3. Данные в первичном пуле хранения на диске ежедневно переносятся в первичный пул хранения на ленте.
4. Данные из пула хранения копий на ленте перемещаются куда-либо вне площадки, чтобы обеспечить поддержку долгосрочного хранения и аварийного восстановления.

Процедура

Чтобы спланировать иерархию пулов хранения, ответьте на следующие вопросы:

a. Какие клиенты должны производить резервное копирование данных на диск и какие клиенты должны производить резервное копирование данных на ленту?
   - Предпочтительный метод - резервное копирование клиентов, на которых находятся большие объекты, например, базы данных, на ленту.
   - Предпочтительный метод - резервное копирование всех остальных клиентов на диск.
   - Для клиентов виртуальных машин (VM) можно производить резервное копирование данных на диск или на ленту. Предпочтительный метод - резервное копирование клиента VM в отдельный дисковый пул хранения, который не переносится на ленту. Если вам нужно перенести клиент VM на ленту, создайте меньший дисковый пул хранения, чтобы на нем находились файлы управления VMware. Для этого меньшего дискового пула хранения нельзя разрешать перенос на ленту. Дополнительную информацию о резервном копировании клиента VM на ленту смотрите в разделах Рекомендации по ленточным устройствам и technote 1239546.

   Совет: Если многим клиентам приходится копировать данные в один пул хранения, рассмотрите возможность использовать пул хранения на диске, так как вы сможете задать много точек монтирования. Вы сможете задать максимальное значение, равное 999, для параметра MAXNUMMP в команде REGISTER NODE.

b. Что следует учесть при назначении емкости пулов хранения на основе диска?

   Как минимум, запланируйте достаточную емкость, чтобы хранить данные за один день операций резервного копирования. Предпочтительный метод - запланировать достаточно емкости, чтобы хранить данные за два дня операций резервного копирования, плюс 20% буфер.

c. Что следует учесть при назначении класса устройств для пула хранения на основе диска?

   Предпочтительный метод - задать класс устройств FILE. Задайте для параметра MOUNTLIMIT значение 4000. Также убедитесь, что у узла достаточно высокое число точек монтирования, которые можно задать, используя параметр MAXNUMMP в команде REGISTER NODE.

d. Нужно ли задавать дедупликацию данных для дискового пула хранения?

   Нет, так как данные хранятся на диске в течение только одного дня, прежде чем данные переносятся на ленту.

e. Следует ли задавать автоматический перенос данных на основе порога переноса?

   Нет. Вместо этого запланируйте ежедневный перенос, используя команду MIGRATE STGPOOL. (Чтобы предотвратить автоматический перенос на основе порога переноса, задайте значение 100 для параметра HIGHMIG и значение 0 для параметра LOWMIG, когда будете вводить команду DEFINE STGPOOL.)

f. Нужно ли задавать задержку переноса?

   Предпочтительный метод - задать ежедневный перенос с диска на ленту и не задавать задержку переноса, для которой требуется дополнительное планирование. Дополнительные сведения о задержках перенастройки смотрите в разделе Перенос файлов в иерахии пулов хранения.

g. Как можно вычислить число лентопротяжных устройств?
   i. Определите собственную скорость перемещения данных накопителем, ознакомившись с документацией производителя. Чтобы получить оценку поддерживаемой скорости передачи данных в среде хранения, вычтите 30% из собственной скорости передачи данных.
   ii. Вычислите нужную скорость поглощения данных сервером. Затем разделите значение на поддерживаемую скорость передачи данных одним ленточным устройством. Результат будет указывать минимальное число накопителей для поддержки поглощения данных.
   iii. Вычислите число точек монтирования, которые требуются клиентам, создающим резервные копии данных на ленте, включая те клиенты, которые используют несколько сеансов. Точки монтирования можно распределить по окну резервного копирования, учитывая, что клиенты, вероятно, производят резервное копирование больших объектов, которые могут использовать большую часть этого окна.
   iv. Вычислите требования к производительности *и* число точек монтирования, которые требуются для выполнения задач по обслуживанию, например, переноса данных с диска на ленту и создания копий с ленты на ленту. Производя резервное копирование данных на ленту, можно избежать обработки переноса, но создание копий с ленты на ленту вдвое увеличит требования к ленточным накопителям.
   v. Вычислите число дополнительных накопителей, которые могут потребоваться, например:
      - Если ленточный накопитель работает неправильно, эта проблема повлияет на число доступных точек монтирования и скорость поглощения данных. Рассмотрите возможность предоставления запасных свободных накопителей. Например, если вам нужно пять ленточных накопителей для обычной работы, рассмотрите возможность предоставить два свободных накопителя.
      - Для операций восстановления и получения могут потребоваться дополнительные ленточные накопители, если вы собираетесь одновременно запускать операции по поглощению данных и обслуживанию. Если потребуется, предоставьте дополнительные ленточные накопители и убедитесь, что они не используются, когда вы запускаете операции восстановления или получения.

h. Какие альтернативы существуют для оптимизации операций восстановления?
   Можно использовать совместное размещение, чтобы повысить производительность системы и оптимизировать организацию данных. При совместном размещении можно сократить число томов, к которым придется обращаться при восстановлении больших объемов данных:
   - В случае пулов хранения на основе дисков предпочтительный метод - это использование совместного размещения по узлам. Сервер размещает данные узла на как можно меньшем числе томов.
   - В случае пулов хранения на основе лент предпочтительный метод - это использование совместного размещения по группам. При совместном размещении по группам сокращается неиспользуемое ленточное пространство, что позволяет совместно разместить на отдельных лентах больше данных.

   Дополнительную информацию о совместном размещении смотрите в разделе Оптимизация операций путем включения совместного размещения файлов клиентов.
   Если вы - опытный системный администратор, вы можете запланировать дополнительные действия для оптимизации операций восстановления. См. разделы Оптимизация операций восстановления для клиентов, Технологии резервного копирования файлов и MOVE NODEDATA (перемещение данных узла в пуле хранения с последовательным доступом).

Хранение данных вне площадки

Чтобы упростить восстановление данных и как часть стратегии аварийного восстановления храните копии лент вне площадки.

Используйте функцию disaster recovery manager (DRM), чтобы сконфигурировать и автоматически сгенерировать план аварийного восстановления, содержащий информацию, сценарии и процедуры, необходимые для автоматического

восстовления сервера и возврата данных клиентов после аварии. Выберите одну следующих возможностей хранения данных вне площадки как стратегию аварийного восстановления для защиты копий лент:

Сохранение вне площадки с одной производственной площадки
: Тома хранения, например, ленточные картриджи и тома носителей, хранятся в расположении вне площадки. Курьер перевозит данные с места хранения вне площадки на площадку восстановления. Если произойдет авария, тома будут отправлены обратно на производственную площадку после восстановления оборудования и сервера IBM Spectrum Protect.

Сохранение вне площадки с площадкой восстановления
: Курьер перевозит тома хранения с производственной площадки туда, где осуществлятся хранение вне площадки. При наличии специальной площадки для восстановления можно сократить время восстановления по сравнению с одной производственной площадкой. Однако при таком способе повышается стоимость восстановления после аварий, так как нужно обслуживать больше аппаратных и программных средств. Например, сайт восстановления должен включать в себя совместимые ленточные устройства и программное обеспечение сервера IBM Spectrum Protect. Для возможности восстановления производственного сайта уже должен быть сконфигурирован и запущен сайт восстановления.

Электронное хранилище
: Чтобы использовать электронное хранилище в качестве стратегии аварийного восстановления, на площадке восстановления должен быть работающий сервер IBM Spectrum Protect. Критические данные с производственного сайта сохраняются на сайте восстановления электронным способом. DRM также используется для хранения некритических данных вне площадки. При электронном сохранении критические данные перемещаются за пределы сайта быстрее и чаще, чем при традиционных способах с использованием курьеров. Время восстановления сокращается, поскольку критические данные уже хранятся на сайте восстановления. Однако, поскольку площадка восстановления работает постоянно, стоимость стратегии аварийного восстановления выше, чем хранение вне площадки.

Понятия, связанные с данным:
Подготовка к аварии и восстановление после аварии с использованием DRM

Планирование защиты

Спланируйте защиту систем в решении IBM Spectrum Protect, используя управление доступом и аутентификацией, и рассмотрите возможность шифрования данных и передачи паролей.

- Планирование ролей администратора
  Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.
- Планирование защищенной связи
  План защиты взаимодействий между компонентами решения IBM Spectrum Protect.
- Планирование хранения зашифрованных данных
  Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите способ, который лучше всего подходит для ваших требований.
- Планирование доступа через брандмауэр
  Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

Планирование ролей администратора

Задайте уровень полномочий, которые вы хотите назначить для решения IBM Spectrum Protect.

Администраторам можно назначить один из следующих уровней полномочий:

Система
: У администраторов с системными полномочиями - высший уровень полномочий. Администраторы с этим уровнем полномочий могут выполнить любую задачу. Они могут управлять всеми доменами политики и пулами хранения и предоставлять полномочия другим администраторам.

Политика
: Администраторы, у которых есть полномочия политики, могут управлять всеми задачами, связанными с управлением политикой. Эти полномочия могут быть неограниченными или могут быть ограничены определенными доменами политики.

Хранение

Администраторы, у которых есть полномочия хранения, могут выделить ресурсы хранения для сервера и управлять ими.

Оператор

Администраторы, у которых есть полномочия оператора, могут управлять непосредственной работой сервера и доступностью таких носителей хранения, как ленточные библиотеки и накопители.

В сценариях в Табл. 1 представлены примеры того, почему вам может потребоваться назначить разные уровни полномочий, чтобы администраторы могли выполнять задачи:

Табл. 1. Сценарии для ролей администраторов

Сценарий	**Тип ID администратора, который нужно задать**
Администратор в небольшой компании управляет сервером и отвечает за все операции сервера.	• Системные полномочия: 1 ID администратора
Администратор нескольких серверов также управляет всей системой. Несколько других администраторов управляют своими собственными пулами хранения.	• Системные полномочия на всех серверах: 1 ID администратора для всех задач по администрированию системы • Полномочия на хранение для назначенных пулов хранения: 1 ID администратора для каждого из других администраторов
Администратор управляет двумя серверами. Другой сотрудник помогает выполнять задачи по администрированию. Два помощника отвечают за то, чтобы производилось резервное копирование важных систем. Каждый помощник отвечает за мониторинг запланированных операций по резервному копированию на одном из серверов IBM Spectrum Protect.	• Системные полномочия на обоих серверах: 2 ID администратора • Полномочия оператора: 2 ID администраторов для помощников с доступом к серверу, за который отвечает каждый сотрудник

Задачи, связанные с данной:
Управление администраторами

Планирование защищенной связи

План защиты взаимодействий между компонентами решения IBM Spectrum Protect.

Определите уровень защиты, требующийся для ваших данных, на основе нормативов и бизнес-требований, которые действуют в вашей компании.

Если для вашего бизнеса требуется высокий уровень защиты паролей и передаваемых данных, запланируйте реализацию защищенной связи на основе протоколов Transport Layer Security (TLS) или Secure Sockets Layer (SSL).

TLS и SSL обеспечивают защищенную связь между сервером и клиентом, но могут отрицательно влиять на производительность системы. Чтобы повысить производительность системы, используйте TLS для аутентификации без шифрования данных объектов. Чтобы указать, использует ли сервер TLS 1.2 для всего сеанса или только для аутентификации, смотрите описание опции клиента SSL для взаимодействий клиента с сервером и параметра UPDATE SERVER=SSL для взаимодействий сервера с сервером. Beginning in V8.1.2, TLS is used for authentication by default. Если вы решите использовать TLS для шифрования всего сеанса, используйте этот протокол только для сеансов, в которых это необходимо, и добавьте на сервер процессорные ресурсы, чтобы справиться с увеличением сетевого трафика. Также можно попробовать использовать другие опции. Например, в некоторых сетевых устройствах, например, в маршрутизаторах и коммутаторах, есть функция TLS или SSL.

TLS и SSL можно использовать для защиты некоторых или всех различных возможных путей связи, например:

- Центр операций: браузер с хабом; хаб с подчиненным сервером
- Клиент с сервером
- Сервер с сервером: репликация узлов

Задачи, связанные с данной:
Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)

Планирование хранения зашифрованных данных

Определите, требуется ли вашей компании шифровать сохраняемые данные, и выберите способ, который лучше всего подходит для ваших требований.

Табл. 1. Выбор метода шифрования данных

Бизнес-требование	**Метод шифрования**	**Дополнительная информация**
Защитите данные на уровне клиентуровень клиента.	Шифрование клиента IBM Spectrum Protect	Данные можно шифровать на уровне файлов, используя список include/exclude. Это позволяет обеспечить высокую степень контроля над тем, какие данные шифруются. На клиенте потребуются дополнительные вычислительные ресурсы, что может повлиять на производительность процессов резервного копирования и восстановления. Дополнительную информацию об этом методе смотрите в разделе Шифрование клиента IBM Spectrum Protect.
Защитите данные в томах пула хранения на ленточном накопителе.	На уровне программы	При использовании метода Приложение IBM Spectrum Protect управляет ключами шифрования для защиты данных в томах пула хранения. Вы должны особо тщательно подходить к защите резервных копий базы данных, так как ключи шифрования хранятся в базе данных сервера. Без доступа к резервным копиям базы данных и без сопоставления ключей шифрования данные восстановить невозможно. Использовать этот метод для шифрования резервных копий базы данных, экспортируемых данных или наборов резервных копий нельзя. Дополнительную информацию о методе Приложение смотрите в разделе Методы шифрования лент.
Защитите данные на ленточном накопителе.	На уровне библиотеки	При использовании метода Библиотека библиотека управляет ключами шифрования. Можно шифровать как данные в пулах хранения, так и другие данные на ленточном накопителе. Вы можете управлять тем, какие тома будут зашифрованы, используя их штрих-коды с серийными номерами. Дополнительную информацию о методе Библиотека смотрите в разделе Методы шифрования лент.
Защитите данные на ленточном накопителе.	На уровне системы	При использовании метода Система шифрованием управляет драйвер устройств или операционная система AIX. Этот метод шифрования доступен только в операционной системе AIX. Можно шифровать как данные в пулах хранения, так и другие данные на ленточном накопителе. Дополнительную информацию о методе Система смотрите в разделе Методы шифрования лент.

Планирование доступа через брандмауэр

Определите, какие у вас заданы брандмауэры и какие порты должны быть открыты, чтобы решение IBM Spectrum Protect работало.

В разделе Табл. 1 описаны порты, используемые сервером, клиентом и компонентом Центр операций.

Табл. 1. Порты, используемые сервером, клиентом и компонентом Центр операций

Элемент	**По умолчанию**	**Направление**	**Описание**
Базовый порт (TCPPORT)	1500	Исходящие/ входящие	Для каждого экземпляра сервера требуется уникальный порт. Можно задать альтернативный номер порта. Опция TCPPORT принимает от клиента как сеансы TCP/IP, так и сеансы с поддержкой SSL. Чтобы задать значения портов для трафика клиента администрирования, можно использовать опцию TCPADMINPORT и опцию ADMINONCLIENTPORT.
SSL-only port (SSLTCPPORT)	Значения по умолчанию нет	Исходящие/ входящие	Этот порт используется, если вы хотите ограничить взаимодействия на порту только сеансами, поддерживающими SSL. Сервер может поддерживать взаимодействия как SSL, так и не SSL, используя опции TCPPORT или TCPADMINPORT.

Элемент	По умолчанию	Направление	Описание
SMB	45	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SSH	22	Входящие/ исходящие	Этот порт используется мастерами конфигурирования, которые, используя собственные протоколы, взаимодействуют с несколькими хостами.
SMTP	25	Исходящие	Этот порт используется для отправки оповещений с сервера по электронной почте.
Репликация	Значения по умолчанию нет	Исходящие/ входящие	Порт и протокол для исходящего порта при репликации заданы командой DEFINE SERVER, которая используется, чтобы настроить репликацию. Входящие порты для репликации - это порты TCP и порты SSL, заданные для исходного сервера в команде DEFINE SERVER.
Порт клиентских расписаний	Порт клиента: 1501	Исходящие	Клиент осуществляет прием на указанном порту и передает номер порта серверу. Сервер соединяется с клиентом, если используется планирование по приглашению сервера. Можно задать альтернативный номер порта в файле опций клиента.
Длительно выполн. сеансы	Параметр KEEPALIVE: YES	Исходящие	Если разрешена опция KEEPALIVE, то контрольные пакеты отправляются во время сеансов клиент-сервер, чтобы не дать программе брандмауэра закрыть длительно выполняющиеся, неактивные соединения.
Центр операций	HTTPS: 11090	Входящие	Эти порты используются для веб-браузера компонента Центр операций. Можно задать альтернативный номер порта.
Порт службы управления клиентами	Порт клиента: 9028	Входящие	Если вы собираетесь использовать компонент Службы управления клиентом IBM Spectrum Protect, порт службы управления клиентами должен быть доступен из компонента Центр операций. Убедитесь, что брандмауэры не запрещают соединения. Служба управления клиентами использует порт TCP сервера клиентского узла для аутентификации, используя административный сеанс.

Задачи, связанные с данной:

Сбор диагностической информации с помощью служб управления клиентами IBM Spectrum Protect

Ссылки, связанные с данной:

опция сервера ADMINONCLIENTPORT

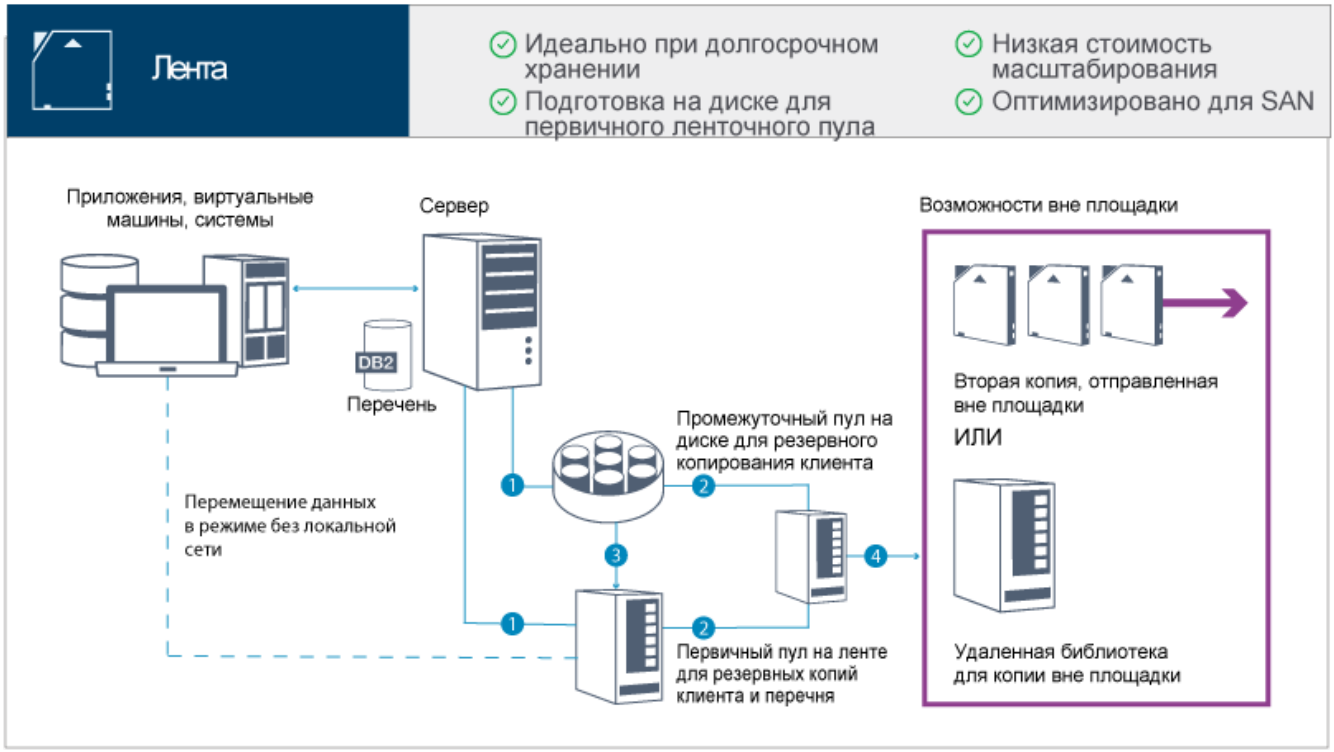
DEFINE SERVER (Задать сервер для обмена данными между серверами)

Опция сервера TCPADMINPORT

опция сервера TCPPORT

Реализация решения по защите данных на основе ленты

Решение на основе ленты использует резервное копирование с диска на диск и на ленту и применяет промежуточное сохранение на диске для оптимизации хранения. Реализуя ленточное решение, можно включить долгосрочное хранение данных и добиться экономичной масштабируемости.



Совет: Описанное решение не включает в себя репликацию узлов. Однако, если вы хотите использовать репликацию узлов, чтобы создать резервную копию пула хранения с диска на диск, убедитесь, что операция репликации завершилась, прежде чем переносить данные с диска на ленту. Репликацию узлов также можно использовать для резервного копирования пула хранения на локальном ленточном устройстве в пул хранения копий на локальном ленточном устройстве.

Путеводитель по реализации

Для настройки решения на основе ленты нужно сделать следующее:

1. Настройте систему
2. Установите сервер и Центр операций.
3. Сконфигурируйте сервер и Центр операций.
4. Подключите ленточные устройства для сервера.
5. Сконфигурируйте ленточные библиотеки для использования сервером.
6. Настройте иерархию пула хранения.
7. Установите и сконфигурируйте клиенты.
8. Сконфигурируйте перемещение данных в режиме без локальной сети.
9. Выберите метод шифрования и сконфигурируйте шифрование.
10. Настройте операции ленточного хранилища.
11. Завершите реализацию.

Настройка системы

Чтобы настроить систему, нужно сначала сконфигурировать дисковое оборудование хранения и серверную систему для IBM Spectrum Protect.

Об этой задаче

Совет: Здесь описаны процедуры настройки сервера и дисковой системы хранения. Чтобы приступить к настройке ленточных устройств, смотрите раздел Подключение ленточных устройств к серверу.

- Конфигурирование оборудования систем хранения
  Чтобы оптимизировать дисковое хранение, прочтите рекомендации по настройке дискового пространства хранения с помощью IBM Spectrum Protect. Затем задайте соединение между сервером и дисковыми устройствами хранения и выполните остальные задачи по конфигурированию.

- Установка операционной системы сервера
  Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.
- Конфигурирование ввода-вывода с несколькими путями
  Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.
- Создание ID пользователя для сервера
  Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.
- Подготовка файловых систем для сервера
  Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

Конфигурирование оборудования систем хранения

Чтобы оптимизировать дисковое хранение, прочтите рекомендации по настройке дискового пространства хранения с помощью IBM Spectrum Protect. Затем задайте соединение между сервером и дисковыми устройствами хранения и выполните остальные задачи по конфигурированию.

Прежде чем начать

Рекомендации по настройке дискового пространства хранения смотрите в разделе Контрольный список для пулов хранения на устройствах DISK или FILE

Процедура

1. Задайте соединение между сервером и устройствами хранения, следуя приведенным ниже рекомендациям:
   - Используйте коммутируемое или прямое усоединение для соединений Fibre Channel.
   - Подберите число портов для соединения и учетную запись для необходимой ширины полосы пропускания.
   - Подберите число портов для соединения на сервере и число портов хоста в дисковой системе.
2. Убедитесь, что драйверы устройств и встроенная микропрограмма в системе сервера, адаптеров и операционной системы, являются современными и находятся на рекомендуемых уровнях.
3. Сконфигурируйте массивы хранения. Убедитесь, что вы правильно произвели планирование, чтобы обеспечить оптимальную производительность. Дополнительную информацию смотрите в разделе Планирование дискового хранилища.
4. Убедитесь, что у системы сервера есть доступ к созданным дисковым томам. Сделайте следующее:
   a. Если система подключена к коммутатору Fibre Channel, произведите зонирование сервера, чтобы увидеть диски.
   b. Отобразите все тома, чтобы сообщить дисковой системе, что данному серверу разрешено видеть каждый диск.
5. Убедитесь, что ленточные и дисковые устройства используют разные порты адаптера шины хоста (Host Bus Adapter, HBA). Управляйте вводом-выводом на ленты и диски с использованием SAN.

Задачи, связанные с данной:
Конфигурирование ввода-вывода с несколькими путями

Установка операционной системы сервера

Установите операционную систему на компьютере сервера и убедитесь, что выполнены требования сервера IBM Spectrum Protect. Скорректируйте параметры операционной системы, как указано.

- Установка в системах AIX
  Выполните следующие действия, чтобы установить AIX в системе сервера.
- Установка в системах Linux
  Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.
- Установка в системах Windows
  Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Установка в системах AIX

Выполните следующие действия, чтобы установить AIX в системе сервера.

Процедура

1. Установите AIX версии 7.1 TL4, SP2 или новее в соответствии с инструкциями производителя.
2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

     ```
     127.0.0.1 localhost
     ```

4. Включите полты выполнения ввода-вывода AIX, введя следующую команду:

   ```
   chdev -l iocp0 -P
   ```

   На производительность сервера может влиять определение часового пояса по Олсону (Olson).
5. Чтобы оптимизировать производительность, измените формат часового пояса с Olson на POSIX. Чтобы обновить параметр часового пояса, используйте следующий формат команды:

   ```
   chtz=локальный_часовой_пояс,дата/время,дата/время
   ```

   Например, если вы находитесь в Тьюсоне (Аризона), где используется стандартное горное время, то вы бы, чтобы перейти к формату POSIX, ввели бы следующую команду:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Добавьте запись в файл .profile пользователя экземпляра, чтобы была задана следующая среда:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Совет: Если пользователь экземпляра недоступен, то выполните этот шаг позже, когда пользователь экземпляра станет доступен.
7. Настройте систему на создание полных файлов ядра приложения. Введите следующую команду:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Чтобы обеспечить взаимодействия с сервером и компонентом Центр операций, убедитесь, что на всех брандмауэрах, которые могут существовать, открыты следующие порты:
   - Для связи с сервером откройте порт 1500.
   - Чтобы обеспечить защищенную связь с компонентом Центр операций, откройте порт 11090 на хаб-сервере.

   Если вы не используете значения портов по умолчанию, то убедитесь, что используемые вами порты открыты.

9. Включите усовершенствования высокой производительности TCP. Введите следующую команду:

   ```
   no -p -o rfc1323=1
   ```

10. Чтобы обеспечить оптимальную пропускную способность и надежность, свяжите вместе четыре порта 10 Gb Ethernet. Используйте инструмент System Management Interface Tool (SMIT), чтобы связать порты друг с другом, используя Etherchannel. При тестировании использовались следующие параметры:

    ```
    режим            8023ad
    auto_recovery    yes             Включить автоматическое восстановление после
                                     передачи управления
    backup_adapter   NONE            Адаптер, используемый при ошибке всего канала
    hash_mode        src_dst_port    Указывает, как выбирается исходящий адаптер
    interval         long            Определяет значение интервала для режима
                                     IEEE 802.3ad
    mode             8023ad          Режим EtherChannel для операции
    netaddr          0               Адрес для команды ping
    noloss_failover  yes             Включает передачу управления без потери данных
                                     после неудачного завершения ping
    num_retries      3               Сколько раз повторять ping, прежде чем заключить
                                     о неудаче
    retry_time       1               Время ожидания (в сек.) между командами ping
    use_alt_addr     no              Включить другой адрес EtherChannel
    use_jumbo_frame  no              Включить фреймы Gigabit Ethernet Jumbo
    ```

11. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 1. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 1. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	**Установка**	**Значение**	**Команда для запроса значения**
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Linux

Выполните следующие действия, чтобы установить Linux x86_64 в системе сервера.

Прежде чем начать

Операционная система устанавливается на внутренних жестких дисках. Сконфигурируйте внутренние жесткие диски, используя аппаратный массив RAID 1. Например, если вы конфигурируете небольшую систему, два внутренних диска по 300 ГБ зеркально отражаются в RAID 1, в результате чего для программы установки операционной системы будет доступен один диск в 300 ГБ.

Процедура

1. Установите Red Hat Enterprise Linux версии 7.1 или новее в соответствии с инструкциями производителя. Получите загрузочный DVD-диск, содержащий Red Hat Enterprise Linux версии 7.1 и запустите свою систему с этого DVD-диска. Опции установки смотрите в приведенных ниже рекомендациях. Если элемент не упомянут в приведенном ниже списке, оставьте для него значение по умолчанию.
    a. После запуска DVD-диска выберите в меню Установить или обновить существующую систему.
    b. В окне с приветствием выберите Проверить этот носитель и установить Red Hat Enterprise Linux 7.1.
    c. Выберите предпочтения языка и клавиатуры.
    d. Выберите свое расположение, чтобы задать нужный часовой пояс.
    e. Выберите Выбор программ, а затем в следующем окне выберите Сервер с графическим пользовательским интерфейсом.
    f. На странице сводной информации установки щелкните по Пункт назначения установки и проверьте следующее:
        - В качестве пункта назначения установки выбирается локальный диск на 300 ГБ.
        - В разделе Другие опции хранения выбирается опция Автоматически сконфигурировать разбиение на разделы.

        Щелкните по Готово.
    g. Щелкните по Начать установку . После запуска установки задайте пароль пользователя root для учетной записи пользователя root.

    По завершении установки перезапустите систему и войдите в систему от имени пользователя root. Введите команду df, чтобы проверить базовое разбиение на разделы. Например, в тест-системе первоначальные разделы выдали следующий результат:

```
[root@tvapp02]# df -h
Файловая сист.                 Размер Исп. Дост. Исп. % Где смонтир.
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G    1%    /dev/shm
tmpfs                   32G   8.8M  32G    1%    /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
   Чтобы обеспечить оптимальную пропускную способность и надежность, рассмотрите возможность связать вместе несколько сетевых портов. Это можно выполнить, создав сетевое соединение Link Aggregation Control Protocol (LACP), которое агрегирует несколько подчиненных портов в одно логическое соединение. Предпочтительный метод состоит в том, чтобы использовать режим связи 802.3ad, параметр miimon, равный 100, и параметр xmit_hash_policy, равный layer3+4.
   Ограничение: Для использования сетевого соединения LACP у вас должен быть сетевой коммутатор, поддерживающий LACP.

   Дополнительные инструкции по конфигурированию привязанных сетевых соединения при использовании Red Hat Enterprise Linux версии 7 смотрите в документе: Создать интерфейс привязки каналов.

3. Откройте файл /etc/hosts и сделайте следующее:
   - Обновите файл, включив в него IP-адрес и имя хоста для сервера. Например:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Убедитесь, что файл содержит запись для localhost с адресом 127.0.0.1. Например:

     ```
     127.0.0.1 localhost
     ```

4. Установите компоненты, необходимые для установки сервера. Выполните описанные ниже шаги, чтобы создать репозиторий Yellowdog Updater Modified (YUM) и установить необходимые пакеты.
   a. Смонтируйте DVD-диск установки Red Hat Enterprise Linux в системном каталоге. Например, чтобы смонтировать его в каталоге /mnt, введите следующую команду:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Убедитесь, что DVD-диск смонтирован, введя команду mount. Должна появиться выходная информация, аналогичная следующему примеру:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Перейдите в каталог репозитория YUM, введя следующую команду:

      ```
      cd /etc/yum/repos.d
      ```

      Если каталог repos.d не существует, создайте его.
   d. Вызовите список содержимого каталога:

      ```
      ls rhel-source.repo
      ```

   e. Переименуйте исходный файл repo, введя команду mv. Например:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Создайте новый файл repo, используя текстовый редактор. Например, чтобы использовать редактор vi, введите следующую команду:

      ```
      vi rhel71_dvd.repo
      ```

   g. Добавьте в новый файл repo следующие строки. Параметр baseurl задает точку монтирования каталога:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h. Установите необходимый пакет ksh.x86_64, введя команду yum. Например:

```
yum install ksh.x86_64
```

Исключительная ситуация: Устанавливать библиотеки compat-libstdc++-33-3.2.3-69.el6.i686 и libstdc++.i686 для Red Hat Enterprise Linux версии 7.1 не нужно.

5. По завершении установки программы вы сможете восстановить исходные значения репозитория YUM, выполнив следующие шаги:
   a. Размонтируйте DVD-диск установки Red Hat Enterprise Linux, введя следующую команду:

   ```
   unmount /mnt
   ```

   b. Перейдите в каталог репозитория YUM, введя следующую команду:

   ```
   cd /etc/yum/repos.d
   ```

   c. Переименуйте созданный вами файл repo:

   ```
   mv rhel71_dvd.repo rhel71_dvd.repo.orig
   ```

   d. Переименуйте исходный файл, используя его исходное имя:

   ```
   mv rhel-source.repo.orig rhel-source.repo
   ```

6. Определите, требуется ли измерения параметров ядра. Сделайте следующее:
   a. Используйте команду sysctl -a, чтобы вывести список значений параметров.
   b. Проанализируйте результаты, следуя рекомендациям в разделе Табл. 1, чтобы определить, не требуются ли какие-либо изменения.
   c. Если требуются изменения, задайте параметры в файле /etc/sysctl.conf. Изменения файлов применяются при запуске системы.

Совет: Автоматически корректируйте значения параметров ядра и устраните необходимость обновления этих параметров вручную. В Linux продукт программное обеспечение баз данных DB2 автоматически корректирует значения параметров ядра взаимодействий между процессами (interprocess communication, IPC) до предпочтительных значений. Чтобы получить дополнительную информацию о значениях параметров ядра, ищите параметры ядра Linux в публикации Документация по продукту DB2 версии 11.1 IBM.

Табл. 1. Оптимальные значения параметра ядра Linux

Параметр	**Описание**
kernel.shmmni	Максимальное число сегментов.
kernel.shmmax	Максимальный размер сегмента совместно используемой памяти (в байтах). Этот параметр нужно задать до автоматического запуска сервера IBM Spectrum Protect при запуске системы.
kernel.shmall	Максимальное число размещенных страниц совместно используемой памяти.
kernel.sem Существует четыре значения для параметра kernel.sem.	(SEMMSL) Максимальное число семафоров на массив.
	(SEMMNS) Максимальное число семафоров на систему.
	(SEMOPM) Максимальное число операций на вызов семафора.
	(SEMMNI) Максимальное число массивов.
kernel.msgmni	Максимальное число очередей сообщений уровня системы.
kernel.msgmax	Максимальный размер сообщения (в байтах).
kernel.msgmnb	Максимальный размер очереди по умолчанию (в байтах).

Параметр	Описание
kernel.randomize_va_space	Параметр kernel.randomize_va_space конфигурирует использование памяти ASLR для ядра. Отключите ASLR, так как это может вызвать ошибки в программе DB2. Дополнительные подробности об ASLR Linux и DB2 смотрите в документе техническое замечание 1365583.
vm.swappiness	Параметр vm.swappiness определяет, может ли ядро выполнять своппинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.
vm.overcommit_memory	Параметр vm.overcommit_memory влияет на то, какой объем виртуальной памяти ядро разрешает выделить. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.

7. Откройте порты брандмауэра для взаимодействия с сервером. Сделайте следующее:
   a. Определите зону, используемую сетевым интерфейсом. По умолчанию, это общедоступная зона.
      Введите следующую команду:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Чтобы использовать адрес порта по умолчанию для взаимодействия с сервером, откройте порт TCP/IP 1500 на брандмауэре Linux.
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Если вы хотите использовать какое-либо значение, отличающееся от значения по умолчанию, вы можете задать число в диапазоне 1024-32767. Если вы откроете порт, отличающийся от порта по умолчанию, вы должны будете указать порт при запуске сценария конфигурирования.

   c. Если вы собираетесь использовать эту систему как хаб, откройте порт 11090, который является портом по умолчанию для защищенных взаимодействий (https).
      Введите следующую команду:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Чтобы изменения вступили в силу, заново загрузите определения брандмауэра.
      Введите следующую команду:

      ```
      firewall-cmd --reload
      ```

8. Убедитесь, что предельные значения для ресурсов процессов пользователя, которые также называются *ulimit*, заданы согласно рекомендациям в разделе Табл. 2. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Табл. 2. Предельные значения для пользователей (ulimit)

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	core	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	данные	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	fsize	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	nofile	65536	`ulimit -Hn`

Тип пользовательского предела	Установка	Значение	Команда для запроса значения
Максимальное время процессора в секундах	cpu	Без ограничений	`ulimit -Ht`
Максимальное число процессов пользователей	nproc	16384	`ulimit -Hu`

Если вам нужно изменить какие-либо предельные значения для пользователей, следуйте инструкциям в документации для вашей операционной системы.

Установка в системах Windows

Установите Microsoft Windows Server 2012 Standard Edition на компьютере-сервере и подготовьте систему к установке и конфигурированию сервера IBM Spectrum Protect.

Процедура

1. Установите Windows Server 2016 Standard Edition, согласно инструкциям изготовителя.
2. Измените политики управления учетными записями Windows, выполнив следующие шаги:
   a. Откройте редактор локальной политики защиты, выполнив secpol.msc.
   b. Выберите Локальные политики > Опции защиты и убедитесь, что отключены следующие политики управления учетными записями пользователей:
      - Режим Утверждать администраторов для встроенной учетной записи Администратор
      - Запускать всех администраторов в режиме Утверждать администраторов
3. Сконфигурируйте параметры TCP/IP согласно инструкциям по установке операционной системы.
4. Примените обновления Windows и включите дополнительные функции, выполнив следующие шаги:
   a. Примените последние обновления Windows Server 2016.
   b. Установите и включите функцию Windows 2012 R2 Microsoft .NET Framework 3.5 при помощи менеджера сервера Windows.
   c. Если потребуется, обновите драйверы устройств FC и Ethernet HBA до новых уровней.
   d. Установите драйвер ввода-вывода с несколькими путями, соответствующий используемой вами дисковой системе.
5. Откройте порт TCP/IP по умолчанию, 1500, для связи с сервером IBM Spectrum Protect. Например, введите следующую команду:

   ```
   netsh advfirewall firewall add rule name="Backup server port 1500"
   dir=in action=allow protocol=TCP localport=1500
   ```

6. На хаб-сервере Центр операций откройте порт по умолчанию для защищенной (https) связи с компонентом Центр операций. Номер порта - 11090. Например, введите следующую команду:

   ```
   netsh advfirewall firewall add rule name="Центр операций port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Конфигурирование ввода-вывода с несколькими путями

Можно разрешить и сконфигурировать поддержку нескольких путей для дискового хранилища. Подробные инструкции смотрите в документации, прилагаемой к вашим аппаратным средствам.

- Системы AIX
  Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.
- Системы Linux
  Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.
- Системы Windows
  Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.

Системы AIX

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.

Процедура

1. Определите адрес порта Fibre Channel, который нужно использовать для определения хоста в дисковой подсистеме. Введите команду lscfg для каждого порта.
   - В небольших и средних системах введите следующие команды:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - В крупных системах введите следующие команды:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Убедитесь, что установлены следующие наборы файлов AIX:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Введите команду cfgmgr, чтобы система AIX пересканировала оборудование и обнаружила доступные диски. Например:

   ```
   cfgmgr
   ```

4. Чтобы вызвать список доступных дисков, введите следующую команду:

   ```
   lsdev -Ccdisk
   ```

   Должна появиться выходная информация следующего вида:

   ```
   hdisk0  Доступно 00-00-00 SAS Дисковый накопитель
   hdisk1  Доступно 00-00-00 SAS Дисковый накопитель
   hdisk2  Доступно 01-00-00 SAS Дисковый накопитель
   hdisk3  Доступно 01-00-00 SAS Дисковый накопитель
   hdisk4  Доступно 06-01-02 MPIO IBM 2076 Диск ФС
   hdisk5  Доступно 07-01-02 MPIO IBM 2076 Диск ФС
   ...
   ```

5. Используйте выходную информацию команды lsdev, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

   Например, ID устройства может быть `hdisk4`. Сохраните список ID устройств для использования при создании файловых систем для сервера IBM Spectrum Protect.

6. Скоррелируйте ID устройств SCSI с LUN отдельных дисков из дисковой системы, перечислив подробную информацию о всех физических томах в системе. Введите следующую команду:

   ```
   lspv -u
   ```

   В системе IBM® Storwize примером того, что показано для каждого устройства, является следующая информация:

   ```
   hdisk4  00f8cf083fd97327  Нет активен
    3321360050763008101057800000000000003004214503IBMfcp
   ```

   В примере значение *600507630081010578000000000000030* - это UID тома, сообщенный интерфейсом управления Storwize.
   Чтобы проверить размер дисков (в мегабайтах) и сравнить его с тем, что указано для системы, введите следующую команду:

   ```
   bootinfo -s hdisk4
   ```

Системы Linux

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.

Процедура

1. Внесите изменения в файл /etc/multipath.conf, чтобы включить поддержку нескольких путей для хостов Linux. Если файл multipath.conf не существует, его можно создать, введя следующую команду:

   ```
   mpathconf --enable
   ```

   В файле multipath.conf при тестировании в системе IBM Storwize были заданы следующие параметры:

   ```
   defaults {
                user_friendly_names no
   }

   devices {
                device {
                            vendor "IBM "
                            product "2145"
                            path_grouping_policy group_by_prio
                            user_friendly_names no
                            path_selector "round-robin 0"
                            prio "alua"
                            path_checker "tur"
                            failback "immediate"
                            no_path_retry 5
                            rr_weight uniform
                            rr_min_io_rq "1"
                            dev_loss_tmo 120
              }
   }
   ```

2. Задайте запуск поддержки нескольких путей при запуске системы. Введите следующие команды:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Чтобы убедиться, что диски видны операционной системе и управляются поддержкой нескольких путей, введите следующую команду:

   ```
   multipath -l
   ```

4. Убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и ID устройств.
   Например, в следующей выходной информации показано, что у диска на 2 ТБ есть две группы путей и четыре активных пути. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула. Используйте часть полного числового ID устройства (в данном примере, 12), чтобы найти том в интерфейсе управления дисковой системой.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   `-+- policy='round-robin 0' prio=0 status=enabled
     |- 1:0:1:18 sdat 66:208  active undef running
     `- 3:0:0:18 sddy 128:0   active undef running
   ```

   a. Если потребуется, исправьте назначения хостов для LUN диска и произведите принудительное пересканирование шины. Например:

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      Также можно перезапустить систему, чтобы пересканировать назначения хостов для LUN дисков.

   b. Убедитесь, что теперь диски доступны для ввода-вывода по нескольким путям, снова введя команду multipath -l.

5. Используйте выходную информацию команды multipath, чтобы найти и представить в виде списка ID устройств для каждого дискового устройства.

   Например, ID устройства для вашего диска в 2 ТБ - это `36005076802810c509800000000000012`.

   Сохраните список ID устройств для использования в следующем шаге.

Системы Windows

Выполните описанные ниже шаги, чтобы включить и сконфигурировать поддержку нескольких путей для дискового хранилища.

Процедура

1. Убедитесь, что установлена функция ввода-вывода по нескольким путям. Если потребуется, установите дополнительные драйверы нескольких путей, связанные с поставщиками.
2. Чтобы убедиться, что диски видны операционной системе и управляются вводом-выводом по нескольким путям, введите следующую команду:

   ```
   c:\program files\IBM\SDDDSM\datapath.exe query device
   ```

3. Ознакомьтесь с выходной информацией для поддержки нескольких путей и убедитесь, что перечислены все устройства и что число путей соответствует ожидаемому. Чтобы определить, какие диски указаны, можно использовать информацию о размере и серийных номерах устройств.
   Например, используя часть полного серийного номера устройства (в данном примере, 34), вы сможете искать том в интерфейсе управления дисковой системой. Размер 2 ТБ подтверждает, что диск соответствует файловой системе пула хранения.

   ```
   № УСТР.   4  ИМЯ УСТРОЙСТВА: Disk5 Part0   ТИП: 2145    ПОЛИТИКА: ОПТИМИЗИРОВАННАЯ
   СЕР.НОМ.: 600507630081010578000000000000034          РАЗМЕР LUN: 2.0 ТБ
   ============================================================================
   № пути       Адаптер/Жесткий диск    Состояние  Режим     Выбор   Ошибки
       0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
       1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
       2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
       3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
   ```

4. Создайте список ID дисковых устройств, используя серийные номера, возвращенные в выходной информации нескольких путей в предыдущем шаге.

   Например, ID устройства для вашего диска в 2 ТБ - это `600507630081010578000000000000034`

   Сохраните список ID устройств для использования в следующем шаге.

5. Чтобы привести новые диски в подключенное состояние и снять атрибут "только для чтения", выполните diskpart.exe со следующими командами. Повторите для каждого из дисков:

   ```
   diskpart
      select Disk 1
      online disk
      attribute disk clear readonly
      select Disk 2
      online disk
      attribute disk clear readonly
      < ... >
      select Disk 49
      online disk
      attribute disk clear readonly
      exit
   ```

Создание ID пользователя для сервера

Создайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. Вы укажете этот ID пользователя при создании экземпляра сервера при первоначальном конфигурировании сервера.

Об этой задаче

В ID пользователя можно использовать только буквы в нижнем регистре (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:

- Длина не должна превышать 8 символов.
- ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
- В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

Процедура

1. Чтобы создать ID пользователя, используйте команды операционной системы.
   - Операционные системы AIXОперационные системы LinuxСоздайте группу и ID пользователя в домашнем каталоге пользователя, который станет владельцем экземпляра сервера.

     Например, чтобы создать ID пользователя tsminst1 в группе tsmsrvrs с паролем tsminst1, введите от имени ID административного пользователя следующие команды:

     Операционные системы AIX

     ```
     mkgroup id=1001 tsmsrvrs
     mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
     passwd tsminst1
     ```

     Операционные системы Linux

     ```
     groupadd tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

     Выйдите из системы, затем снова в нее войдите. Перейдите на созданную вами учетную запись пользователя. Используйте интерактивную программу входа в систему, например, telnet, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.
   - Операционные системы WindowsСоздайте ID пользователя, а затем добавьте новый ID в группу администраторов. Например, чтобы создать ID пользователя tsminst1, введите следующую команду:

     ```
     net user tsminst1 * /add
     ```

     После создания и проверки пароля для нового пользователя добавьте ID пользователя в группу Администраторы, введя следующие команды:

     ```
     net localgroup Administrators tsminst1 /add
     net localgroup DB2ADMNS tsminst1 /add
     ```

2. Завершите сеанс для нового ID пользователя.

Подготовка файловых систем для сервера

Чтобы дисковое хранилище использовалось сервером, нужно выполнить конфигурирование файловой системы.

- Подготовка файловых систем в системах AIX
  Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.
- Подготовка файловых систем в системах Linux
  Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.
- Подготовка файловых систем в системах Windows
  Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Подготовка файловых систем в системах AIX

Вы должны создать группы томов, логические тома и файловые системы для сервера, используя менеджер логических томов AIX.

Процедура

1. Увеличьте глубину очереди и максимальный размер передачи для всех доступных дисков *hdiskX*. Введите для каждого диска следующие команды:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Не выполняйте эти команды для внутренних дисков операционной системы, например, для *hdisk0*.
2. Создайте группы томов для базы данных, активного журнала, архивного журнала, резервного копирования базы данных и пула хранения IBM Spectrum Protect. Введите команду mkvg, указав ID устройств для соответствующих дисков, которые вы указали ранее.
   Например, если имена устройств *hdisk4, hdisk5* и *hdisk6* соответствуют дискам базы данных, включите их в группу томов базы данных и т.д.
   Размер системы: Приведенные ниже команды основаны на конфигурации системы среднего размера. Для малых и больших систем необходимо соответствующим образом настроить синтаксис.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Определите имена физического тома и число свободных физических разделов, которые следует использовать при создании логических томов. Введите команду lsvg для каждой группы томов, которую вы создали в предыдущем шаге.
   Например:

   ```
   lsvg -p tsmdb
   ```

   Вывод будет подобен следующему. В столбце *FREE PPs* представлены свободные физические разделы:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Создайте логические тома в каждой группе томов при помощи команды mklv. Размер томов, группа томов и имена устройств будут разными в зависимости от размера вашей системы и различий в конфигурации дисков.
   Например, чтобы создать тома для базы данных IBM Spectrum Protect в системе среднего размера, введите следующие команды:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Сформатируйте файловые системы на каждом логическом томе, используя команду crfs.
   Например, чтобы сформатировать файловые системы для базы данных в системе среднего размера, введите следующие команды:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Смонтируйте все заново созданные файловые системы, введя следующую команду:

   ```
   mount -a
   ```

7. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере выходной информации команды показано, что объем используемого пространства, как правило, составляет 1%:

```
tapsrv07> df -g /tsminst1/*
Файловая сист. Блоки ГБ   Свободно  % исп. Мое исп. % моего исп. Смонтировано
/dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
```

8. Убедитесь, что у ID пользователя, созданного в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам на сервере.

Подготовка файловых систем в системах Linux

Файловые системы ext4 или xfs следует сформатировать на каждом из LUN диска, которые будет использовать сервер IBM Spectrum Protect.

Процедура

1. Используя список ID устройств, сгенерированный ранее, введите команду mkfs, чтобы создать и сформатировать файловую систему для каждого устройства LUN хранения. Укажите ID устройства в команде. Смотрите следующую таблицу. Для базы данных сформатируйте файловые системы ext4:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Для LUN пула хранения сформатируйте файловые системы xfs:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Команду mkfs можно вводить до 50 раз в зависимости от того, сколько разных устройств у вас есть.

2. Создайте каталоги точек монтирования для файловых систем.

   Введите команду mkdir для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования.

   Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

   ```
   mkdir /tsminst1
   ```

   Повторите команду mkdir для каждой файловой системы.
3. Добавьте в файл /etc/fstab запись для каждой файловой системы, чтобы файловые системы монтировались автоматически при запуске сервера.
   Например:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Смонтируйте файловые системы, которые вы добавили в файл /etc/fstab, введя команду mount -a.
5. Вызовите список всех файловых систем, введя команду df. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Проверьте также доступное пространство. В следующем примере в системе IBM® Storwize показано, что объем используемого пространства, как правило, составляет 1%:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Файловая сист.                                  Размер Исп. Дост. Исп. % Где смонтир.
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```

6. Убедитесь, что у ID пользователя, созданного в разделе Создание ID пользователя для сервера, есть права доступа для чтения и записи к каталогам на сервере IBM Spectrum Protect.

Подготовка файловых систем в системах Windows

Вы должны сформатировать файловые системы New Technology (NTFS) на каждом из LUN дисков, которые будут использоваться сервером IBM Spectrum Protect.

Процедура

1. Создайте каталоги точек монтирования для файловых систем.

Введите команду md для каждого каталога, который вы должны создать. Используйте значения каталогов, записанные вами в рабочих таблицах планирования. Например, чтобы создать каталог экземпляра сервера, используя значение по умолчанию, введите следующую команду:

```
md c:\tsminst1
```

Повторите команду md для каждой файловой системы.

2. Создайте том для каждого LUN диска, отображенного в каталог в каталоге экземпляра сервера с использованием менеджера томов Windows.

   Выберите Менеджер серверов > Службы файлов и хранения и выполните описанные ниже шаги для каждого диска, соответствующего отображению LUN, созданному в предыдущем шаге:

   a. Переведите диск в подключенное состояние.
   b. Инициализируйте диск до базового типа GPT, который является типом по умолчанию.
   c. Создайте простой том, занимающий все пространство на диске. Сформатируйте файловую систему с использованием NTFS и задайте метку, соответствующую назначению тома, например, TSMfile00. Не назначайте для нового тома букву диска. Вместо этого отобразите том в каталог в каталоге экземпляра, например, в C:\tsminst1\TSMfile00.
      Совет: Определите метку тома и метки отображений каталога на основе сообщенного размера диска.
3. Убедитесь, что файловые системы смонтированы с использованием правильного LUN и правильной точки монтирования. Вызовите список всех файловых систем, введя команду mountvol и ознакомившись с выходной информацией. Например:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```

4. По завершении конфигурирования диска перезапустите систему.

Дальнейшие действия

Вы можете подтвердить объем свободного пространства для каждого тома, используя Проводник Windows.

Установка сервера и компонента Центр операций

Используйте для установки компонентов графический мастер IBM® Installation Manager.

- Установка в системах AIX и Linux
  Установите сервер IBM Spectrum Protect и Центр операций в той же системе.
- Установка в системах Windows
  Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Установка в системах AIX и Linux

Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Прежде чем начать

Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

1. Операционные системы AIXУбедитесь, что у вас в системе установлены необходимые файлы RPM.

   Дополнительные сведения смотрите в разделе Установка обязательных файлов RPM для графического мастера.

2. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042992.
3. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
4. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

```
chmod a+x имя_пакета.bin
```

5. Извлеките пакет, введя следующую команду:

   ```
   ./имя_пакета.bin
   ```

   где *имя_пакета* - это имя скачанного файла.
6.  Операционные системы AIXУбедитесь, что включена следующая команда, чтобы мастера работали правильно:

   ```
   lsuser
   ```

   По умолчанию эта команда включена.
7. Перейдите в каталог, куда вы поместили исполняемый файл.
8. Запустите мастер установки, введя следующую команду:

   ```
   ./install.sh
   ```

   Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

- Установка обязательных файлов RPM для графического мастера
  Файлы RPM необходимы для графического мастера IBM Installation Manager.

Установка в системах Windows

Установите сервер IBM Spectrum Protect и Центр операций в той же системе.

Прежде чем начать

Убедитесь, что выполнены следующие обязательные требования:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
- Убедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

1. Прежде чем скачивать пакет установки, убедитесь, что у вас достаточно места для хранения файлов установки после их извлечения из пакета продукта. Требования к пространству смотрите в документе по скачиванию по адресу: техническое замечание 4042993.
2. Перейдите на страницу Passport Advantage и скачайте файл пакета в пустой каталог по вашему выбору.
3. Перейдите в каталог, куда вы поместили исполняемый файл.
4. Дважды щелкните по выполняемому файлу, чтобы извлечь его в текущий каталог.
5. В каталоге, куда были распакованы файлы установки, запустите мастер установки, дважды щелкнув по файлу install.bat. Выбирая пакеты для установки, выберите и сервер, и Центр операций.

Дальнейшие действия

- Если в процессе установки возникнут ошибки, они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager.

Чтобы просмотреть файлы журнала установки в инструменте Installation Manager, выберите Файл > Просмотреть журнал. Чтобы собрать эти файлы журналов из инструмента Installation Manager, выберите Справка > Экспорт данных для анализа ошибок.

- После установки сервера и до его настройки к работе посетите сайт сайт поддержки IBM Spectrum Protect. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Конфигурирование сервера и компонента Центр операций

После установки компонентов выполните конфигурирование сервера IBM Spectrum Protect и компонента Центр операций.

- Конфигурирование экземпляра сервера
  Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.
- Установка клиента резервного копирования и архивирования
  Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.
- Как задать опции для сервера
  Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.
- Понятия, касающиеся защиты
  Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.
- Конфигурирование Центра операций
  После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.
- Регистрация лицензии на продукт
  Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.
- Как задать правила хранения данных для вашего бизнеса
  После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.
- Как задать расписания для операций по обслуживанию сервера
  Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.
- Определение расписаний клиентов
  Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Конфигурирование экземпляра сервера

Используйте мастер конфигурирования экземпляра сервера IBM Spectrum Protect, чтобы выполнить первоначальное конфигурирование сервера.

Прежде чем начать

Убедитесь, что выполнены следующие требования:
 Операционные системы AIX  Операционные системы Linux

- В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
- В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле sshd_config в каталоге /etc/ssh/. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения *localhost*.
- Вы должны иметь возможность войти в IBM Spectrum Protect, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
- Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Операционные системы WindowsУбедитесь, что служба удаленного реестра запущена, выполнив следующие шаги:

1. Выберите Пуск > Администрирование > Службы. В окне Службы выберите Удаленный реестр. Если служба не запущена, щелкните по Пуск.
2. Убедитесь, что порты 137, 139 и 445 не заблокированы брандмауэром:
   a. Щелкните по Запуск > Панель управления > Брандмауэр Windows.
   b. Выберите Дополнительные параметры.
   c. Выберите Входные правила.
   d. Выберите Новое правило.
   e. Создайте правило порта для портов TCP 137, 139 и 445, чтобы разрешить соединения для доменных и частных сетей.
3. Сконфигурируйте управление учетными записями пользователей, получив доступ к опциям Локальная политика безопасности и выполнив следующие шаги:
   a. Щелкните по Пуск > Администрирование > Локальная политика безопасности. Разверните Локальные политики > Опции безопасности.
   b. Если эта возможность еще не включена, включите встроенную учетную запись администратора, выбрав Учетные записи: Состояние учетной записи администратора > Включить > ОК.
   c. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для всех администраторов Windows, выбрав Управление учетными записями пользователей: Запускать всех администраторов в режиме утверждения администраторов > Выключить > ОК.
   d. Если эта возможность еще не выключена, выключите управление учетными записями пользователей для встроенной учетной записи администратора, выбрав Управление учетными записями пользователей: Режим утверждения администраторов для встроенной учетной записи администратора > Выключить > ОК.
4. Если вы изменили какие-либо парамптры в предыдущих шагах, перезапустите сервер, прежде чем приступать к работе с мастером конфигурирования.

Об этой задаче

Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

Процедура

1. Запустите локальную версию мастера.
   - Операционные системы AIXОперационные системы LinuxОткройте программу dsmicfgx в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запустить только от имени пользователя root.
   - Операционные системы WindowsЩелкните по Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования.
2. Завершите конфигурирование, следуя инструкциям. Используйте информацию, записанную вами в таблицу Рабочие листы планирования в ходе настройки системы IBM Spectrum Protect, чтобы задать каталоги и опции в мастере.

   Операционные системы AIXОперационные системы LinuxВ окне Информация о сервере задайте автоматический запуск сервера при загрузке системы, используя ID пользователя экземпляра.

   Операционные системы WindowsПри использовании мастера конфигурирования для сервера будет задан автоматический запуск при перезагрузке.

Установка клиента резервного копирования и архивирования

Лучше всего установить клиент резервного копирования и архивирования IBM Spectrum Protect в серверной системе, чтобы были доступны административный клиент командной строки и планировщик.

Процедура

Чтобы установить клиент резервного копирования и архивирования, выполните инструкции по установке для вашей операционной системы.

- Установить клиентов резервного копирования и архивирования UNIX и Linux
- Первая установка клиента Windows

Как задать опции для сервера

Проверьте файл опций сервера, установленный вместе с сервером IBM Spectrum Protect, чтобы убедиться, что заданы правильные значения для вашей системы.

Процедура

1. Перейдите в каталог экземпляра сервера и откройте файл dsmserv.opt.
2. Ознакомьтесь со следующими значениями в таблице и проверьте параметры опций сервера на основе размера системы.

Серверный параметр	**Значение**
ACTIVELOGDIRECTORY	Путь каталога, заданный во время конфигурации
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	Нет
ARCHLOGDIRECTORY	Путь каталога, заданный во время конфигурации
COMMMETHOD	TCPIP
COMMTIMEOUT	3600
DEVCONFIG	devconf.dat
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	volhist.dat

Обновите параметры опций сервера, если потребуется, чтобы они соответствовали значениям в таблице. Чтобы внести обновления, закройте файл dsmserv.opt и воспользуйтесь командой SETOPT в интерфейсе командной строки администрирования, чтобы задать опции.
Например, чтобы обновить опцию IDLETIMEOUT до 60, введите следующую команду:

```
setopt idletimeout 60
```

3. Чтобы сконфигурировать защищенную связь с сервером, клиентами и Центр операций, то проверьте опции в следующей таблице:

Серверный параметр	**Системы всех размеров**
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPORT	Задайте номер порта SSL. Драйвер связи TCP/IP сервера ожидает на этом порту поступления от клиента требований об установлении сеансов с поддержкой SSL.
SSLTCPADMINPORT	Задайте адрес порта, на котором сервер ожидает требований установления сеансов SSL от клиента администрирования с интерфейсом командной строки.
SSLTLS12	YES

Если нужно обновить любое из значений опций, измените файл dsmserv.opt, используя следующие рекомендации:
   - Чтобы включить опцию, удалите звездочку в начале строки.
   - В каждой строке введите только одну опцию и заданное для нее значение.
   - Если опция встречается в нескольких записях в файле, сервер будет использовать последнюю запись.

Сохраните свои изменения файл и закройте файл. Если вы непосредственно внесете изменения в файл dsmserv.opt, вы должны будете перезапустить сервер, чтобы изменения вступили в силу.

Понятия, касающиеся защиты

Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.

Transport Layer Security

Можно использовать протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS), чтобы обеспечить защиту транспортного слоя для безопасной связи между серверами, клиентами и агентами хранения. Если вы пересылаете данные между сервером, клиентом и агентом хранения, используйте SSL или TLS для шифрования данных.

Совет: Любая документация IBM Spectrum Protect, обозначенная как "SSL" или "выбрать SSL", применима к TLS.

SSL предоставляется Global Security Kit (GSKit), установленным с сервером IBM Spectrum Protect и используемым сервером, клиентом и агентом хранения.

Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных DB2, который используется какими-либо серверами IBM Spectrum Protect.

Каждый сервер, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатором (certificate authority, CA). Вы можете использовать свои собственные сертификаты или можете приобрести сертификаты у сертификатора (CA). Любой сертификат нужно установить и добавить к базе данных ключей для сервера IBM Spectrum Protect, клиента или агента хранения. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL. Некоторые сертификаты сертификаторов предварительно устанавливаются в базах данных ключей по умолчанию.

SSL устанавливается независимо от сервера IBM Spectrum Protect, клиента и агента хранения.

Уровни полномочий

При использовании каждого сервера IBM Spectrum Protect существует ряд доступных уровней административных полномочий, определяющих задачи, которые может выполнить администратор.

После регистрации администратору нужно предоставить полномочия, назначив для него один или несколько уровней административных полномочий. Администратор с системными полномочиями может выполнить любую задачу с сервером и назначить уровни полномочий для других администраторов, воспользовавшись командой GRANT AUTHORITY. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Администратор может зарегистрировать другие ID администраторов, предоставить им уровни полномочий, переименовать или удалить их, а также блокировать или разблокировать их доступ к серверу.

Администратор может управлять доступом к определенным клиентским узлам для ID пользователей root и ID пользователей, не являющихся пользователями root. По умолчанию, ID пользователя, не являющегося пользователем root, не может производить резервное копирование данных на узле. Используйте команду UPDATE NODE, чтобы изменить параметры узла и включить резервное копирование.

Пароли

По умолчанию сервер автоматически использует аутентификацию с помощью пароля. Если аутентификация пароля включена (on), все пользователи при получении доступа к серверу должны указывать пароль.

Используйте Lightweight Directory Access Protocol (LDAP), чтобы применить более строгие требования к паролям. Дополнительную информацию смотрите в разделе Управление паролями и процедурами входа (V7.1.1).

Табл. 1. Характеристики аутентификации паролей

Характеристика	**Дополнительная информация**
Значение регистра символов	Без учета регистра.

Характеристика	Дополнительная информация
Срок действия пароля по умолчанию	90 дней. Отсчет начинается с момента первой регистрации на сервере ID администратора или клиентского узла. Если в течение этого периода пароль не изменится, пароль нужно будет изменить, когда пользователь в следующий раз получит доступ к серверу.
Число попыток ввода неправильного пароля	Для всех клиентских узлов можно установить максимальное количество последовательных попыток неправильного ввода пароля. После превышения данного значения сервер блокирует такой узел.
Длина пароля по умолчанию	8 символов Администратор может задать минимальную длину. Начиная с версии 8.1.4, минимальная длина паролей сервера по умолчанию изменилась с 0 до 8 символов.

Защита сеанса

Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами и назначается с использованием параметра SESSIONSECURITY.

Для параметра SESSIONSECURITY можно задать одно из следующих значений:

- Значение STRICT принудительно применяет наиболее высокий уровень защиты взаимодействий между серверами IBM Spectrum Protect, узлами и администраторами.
- Значение TRANSITIONAL указывает, что при обновлении программы IBM Spectrum Protect до V8.1.2 или новее используется существующий протокол связи. Это значение по умолчанию. Если задано SESSIONSECURITY=TRANSITIONAL, автоматически применяются более строгие параметры защиты при использовании более высоких версий протокола TLS и при обновлении программы до V8.1.2 или новее. После того как узел, администратор или сервер будет соответствовать требованиям для значения STRICT, защита сеанса автоматически обновится до значения STRICT, и объект больше не сможет проходить аутентификацию, исплользуя предыдущую версию клиента или более ранние протоколы TLS.
  Прим.: До обновления серверов обновлять клиенты резервного копирования и архивирования до V8.1.2 или новее не нужно. После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжат взаимодействовать с сервером, используя значение TRANSITIONAL, пока объект будет соответствовать требованиям для значения STRICT. Точно так же можно обновить клиенты резервного копирования и архивирования до V8.1.2 или новее до обновления серверов IBM Spectrum Protect, но обновлять серверы сначала не требуется. Связь между серверами и клиентами не прерывается.

Дополнительные сведения о значениях параметра SESSIONSECURITY смотрите в описаниях следующих команд.

Табл. 2. Команды, используемые, чтобы задать параметр SESSIONSECURITY

Объект	Команда
Клиентские узлы	• REGISTER NODE • UPDATE NODE
Администраторы	• REGISTER ADMIN • UPDATE ADMIN
Серверы	• DEFINE SERVER • UPDATE SERVER

Администраторы, прошедшие аутентификацию с использованием команды DSMADMC, команды DSMC или программы dsm, после аутентификации с использованием V8.1.2 или новее не смогут проходить аутентификацию с использованием более ранней версии. Чтобы устранить проблемы аутентификации администраторов, смотрите следующие советы:
Советы:

- Убедитесь, что все программы IBM Spectrum Protect, используемые учетной записью администратора для входа в систему, обновлены до V8.1.2 или новее. Если учетная запись администратора производит вход из нескольких систем, убедитесь, что сертификат сервера установлен в каждой системе.
- После того как администратор пройдет аутентификацию на сервере V8.1.2 или новее, используя клиент V8.1.2 или новее, администратор сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. Команду администратора можно вводить из любой системы.
- Если потребуется, создайте отдельную учетную запись администратора, чтобы использовать ее только при работе с клиентами и серверами, на которых работает V8.1.1 или более ранняя программа.

Принудительно примените наивысший уровень защиты взаимодействий с сервером IBM Spectrum Protect, сделав так, чтобы все узлы, администраторы и серверы использовали защиту сеанса STRICT. Можно воспользоваться командой SELECTЮ чтобы определить, какие серверы, узлы и администраторы используют защиту сеанса TRANSITIONAL, чтобы их обновить для использования защиты сеанса STRICT.

- Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)
  Чтобы шифровать данные и защищать связь в вашей среде, на сервере и на клиенте резервного копирования и архивирования IBM Spectrum Protect включен протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Сертификат SSL используется для проверки требований связи между сервером и клиентом.

Задачи, связанные с данной:
Защита связи

Конфигурирование Центра операций

После установки компонента Центр операций выполните описанные ниже действия по конфигурированию, чтобы начать управлять средой хранения.

Прежде чем начать

Если вы подключаетесь к компоненту Центр операций впервые, вы должны предоставить следующую информацию:

- Информация о соединении для сервера, который вы хотите назначить хаб-сервером
- Идентификационные данные входа в систему для администратора, который задан для этого сервера

Процедура

1. Определите хаб-сервер. Введите в окне веб-браузера следующий адрес:

   `https://`*`имя_хоста`*`:`*`защищенный_порт`*`/oc`

   Здесь используются следующие обозначения:
   - *имя_хоста* - это имя компьютера, где установлен компонент Центр операций
   - *защищенный_порт* - это номер порта, используемого компонентом Центр операций для HTTPS-взаимодействий на этом компьютере

   Например, если имя хоста - это tsm.storage.mylocation.com и вы используете для компонента Центр операций защищенный порт по умолчанию, адрес пример следующий вид:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

   Когда вы впервые входите в компонент Центр операций, мастер поможет вам выполнить первоначальное конфигурирование, чтобы задать нового администратора с системными полномочиями на сервере.

2. Настройте защищенные взаимодействия между компонентом Центр операций и хаб-сервером, сконфигурировав протокол Secure Sockets Layer (SSL).

   Следуйте инструкциям в разделе Защита связи между компонентом Центр операций и хаб-сервером.

3. Необязательно: Чтобы ежедневно получать по электронной почте отчет, в котором суммируется состояние системы, сконфигурируйте параметры электронной почты в компоненте Центр операций.

   Следуйте инструкциям в разделе Состояние системы отслеживания с использованием отчетов по электронной почте.

- Защита связи между компонентом Центр операций и хаб-сервером
  Для защиты связи между компонентом Центр операций и хаб-сервером добавьте сертификат Transport Layer Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Регистрация лицензии на продукт

Чтобы зарегистрировать лицензию для продукта IBM Spectrum Protect, используйте команду REGISTER LICENSE.

Об этой задаче

Лицензии хранятся в файлах сертификата регистрации, который содержит сведения о лицензировании для продукта. Файлы регистрационных сертификатов находятся на носителе установки и при установке помещаются на сервер. После регистрации продукта лицензии хранятся в NODELOCK-файле в текущем каталоге.

Процедура

Зарегистрируйте лицензию, указав имя файла сертификата регистрации, содержащего лицензию. Чтобы использовать построитель команд Центр операций для этой задачи, выполните следующие шаги:

1. Откройте Центр операций.
2. Откройте построитель команд компонента Центр операций, установив указатель мыши на значок параметров и щелкнув по Построитель команд.
3. Введите команду REGISTER LICENSE. Например, чтобы зарегистрировать базовую лицензию IBM Spectrum Protect, введите следующую команду:

   ```
   register license file=tsmbasic.lic
   ```

Дальнейшие действия

Сохраните носитель установки, на котором содержатся файлы сертификата регистрации. Возможно, вам придется снова зарегистрировать лицензию, если, например, возникнет одно из следующих условий:

- Сервер перенесен на другой компьютер;
- Файл NODELOCK поврежден. Сервер сохраняет данные лицензий в файле NODELOCK, расположенном в каталоге, из которого запускается сервер.
- Операционные системы LinuxВы изменяете микросхему процессора, связанную с сервером, на котором установлен сервер.

Как задать правила хранения данных для вашего бизнеса

После создания пула хранения каталога-контейнера для дедупликации данных обновите политику сервера по умолчанию, чтобы использовать новый пул хранения. В мастере Добавить пул хранения откроется страница Службы в компоненте Центр операций, чтобы можно было выполнить эту задачу.

Процедура

1. На странице Службы в Центр операций выберите домен STANDARD и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики. На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.
3. Щелкните по переключателю Конфигурировать и внесите следующие изменения:
   - Измените объект назначения резервного копирования для класса управления STANDARD, задав пул хранения каталога-контейнера.
   - Измените значение в столбце Резервные копии на Без ограничения.
   - Измените срок хранения. Задайте в столбце Хранить лишние резервные копии значение 30 дней или более в зависимости от ваших бизнес-требований.
4. Сохраните изменения и щелкните по переключателю Конфигурировать, чтобы набор политик стал недоступен для изменения.
5. Активируйте набор политик, для чего щелкните по Активировать.

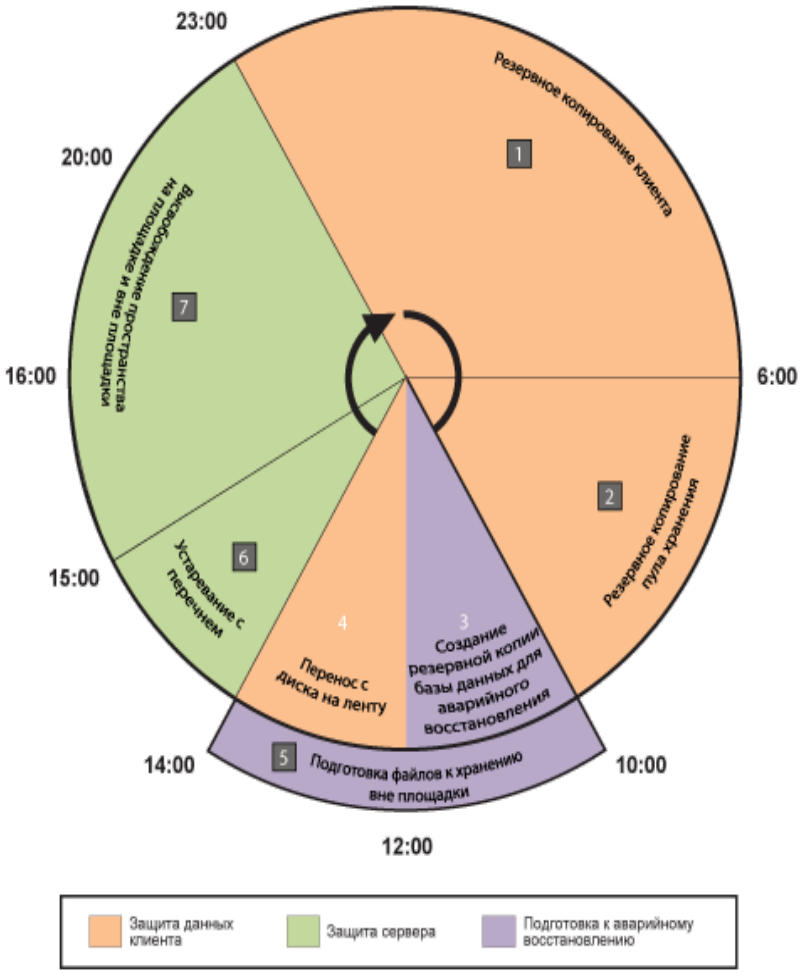
Как задать расписания для операций по обслуживанию сервера

Создайте расписания для каждой операции по обслуживанию сервера, используя команду DEFINE SCHEDULE в построителе команд компонента Центр операций.

Об этой задаче

Запланируйте операции обслуживания сервера, так чтобы они выполнялись после операций резервного копирования клиента. Вы можете управлять синхронизацией расписаний, задав время начала в сочетании с длительностью каждой операции.

На следующем рисунке приводится пример того, как спланировать операции обслуживания.
Рис. 1. Ежедневное расписание операций сервера для ленточного решения



В приведенной ниже таблице показано, как можно запланировать процессы обслуживания сервера в сочетании с расписанием резервного копирования клиента для ленточного решения.

Операция	**Запланированное задание**
Резервное копирование клиента	Начинается в 23:00.
Резервное копирование пула хранения	Начинается в 06:00.

Операция	Запланированное задание
Обработка базы данных и файлов аварийного восстановления	• Операция резервного копирования базы данных начинается в 10:00 или через 11 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения. • Информация о конфигурации устройства и резервное копирование хронологии томов запускаются в 17:00 или спустя 7 часов после запуска операций резервного копирования базы данных. • Удаление хронологии томов запускается в 20:00 или спустя 10 часов после запуска операции резервного копирования базы данных.
Подготовка файлов для хранения вне сайта	Начинается в 10:00, одновременно с началом обработки базы данных и файлов аварийного восстановления.
Перенастройка с диска для записи на ленту	Начинается в 12:00 или через 2 часа после запуска операции резервного копирования базы данных.
Устаревание инвентарного перечня	Начинается в 14:00 или через 15 часов после начала операции резервного копирования клиента. Этот процесс выполняется до его завершения.
Восстановление пространства	Начинается в 15:00 или через 16 часов после начала операции резервного копирования клиента.

Процедура

После того как вы сконфигурируете класс устройств для резервных копий базы данных, создайте расписания для резервного копирования базы данных и других необходимых операций обслуживания, используя команду DEFINE SCHEDULE. В зависимости от размера вашей среды вам, возможно, придется скорректировать время запуска для каждого расписания в примере.

1. Задайте класс устройств для операции резервного копирования, прежде чем создавать расписание для резервного копирования базы данных. Используйте команду DEFINE DEVCLASS, чтобы создать класс устройств с именем LTOTAPE:

   ```
   define devclass ltotape devtype=lto library=ltolib
   ```

2. Задайте класс устройств для автоматического резервного копирования базы данных. Используйте команду SET DBRECOVERY, чтобы указать класс устройств, созданный вами для резервного копирования базы данных в предыдущем шаге. Например, если класс устройств - это LTOTAPE, введите следующую команду:

   ```
   set dbrecovery ltotape
   ```

3. Создайте расписания для операций обслуживания, используя команду DEFINE SCHEDULE. Обязательные операции с примерами команд смотриет в следующей таблице.

Операция	Примеры команд и дополнительная информация
Создайте резервные копии пулов хранения.	Создайте расписание, чтобы выполнить команду BACKUP STGPOOL. Например, введите следующую команду, чтобы создать расписание резервного копирования для первичного пула хранения с именем PRIMARY_POOL. Резервное копирование пула будет производиться в пул хранения копий, COPYSTG: `define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1`

Операция	Примеры команд и дополнительная информация
Создайте резервную копию базы данных.	Создайте расписание, чтобы выполнить команду BACKUP DB. Например, введите следующую команду, чтобы создать расписание резервного копирования, использующее новый класс устройств: `define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Создать рез. копию базы данных." startdate=today starttime=10:00:00 duration=45 durunits=minutes`
Реплицируйте узлы.	(Необязательно) Используйте репликацию узлов для защиты данных клиентов путем резервного копирования данных на вторичный сервер. Инструкции смотрите в разделе Репликация данных клиента на другой сервер. Прежде чем приступать к операциям по переносу, убедитесь, что репликация узлов выполнена.
Переносите данные с диска на ленту ежедневно.	Создайте расписание для переноса пула хранения. Например, если имя дискового пула хранения - DISKPOOL, а имя следующего пула хранения - TAPEPOOL, вы можете запланировать перенос пула хранения, введя следующую команду: `define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days` Чтобы довести пропускную способность до максимума, можно задать число параллельных процессов, которые следует использовать для переноса файлов, выполнив следующие шаги: a. В случае ленточного пула хранения убедитесь, что включено совместное размещение. Чтобы проверить, включено ли совместное размещение, введите команду QUERY STGPOOL. Убедитесь, что в поле `COLLOCATE` задано значение `GROUP`, `NODE` или `FILESPACE`. Если значение `GROUP`, `NODE` или `FILESPACE` не задано, используйте команду UPDATE STGPOOL, чтобы задать `COLLOCATE=GROUP`, `COLLOCATE=NODE` или `COLLOCATE=FILESPACE` в зависимости от конфигурации вашей системы. b. Для дискового пула хранения используйте команду DEFINE STGPOOL или UPDATE STGPOOL, чтобы задать значение для параметра MIGPROCESS. Например, если у вас есть 12 ленточных накопителей, задайте `MIGPROCESS=10`. Таким образом для процессов переноса будет использоваться число ленточных накопителей, достигающее 10. Два накопителя резервируются для других задач, например, операций восстановления, резервного копирования базы данных и резервного копирования клиента.

Операция	Примеры команд и дополнительная информация
Подготовьте файлы для хранения вне сайта.	a. Переместите ленточные тома куда-либо вне площадки, следуя инструкциям в разделе Перемещение носителей резервных копий. b. Создайте файл плана аварийного восстановления, введя команду PREPARE на исходном сервере: `prepare` c. Убедитесь, что все тома, которые требуются для восстановления после аварий, включены в файл плана восстановления. Дополнительные сведения смотрите в разделе Подготовка к аварии и восстановление после аварии с использованием DRM.
Создайте резервную копию информации о конфигурации устройств.	Создайте расписание, чтобы выполнить команду BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Создать рез. копию файла конфигурации устройства." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Создайте резервную копию хронологии томов.	Создайте расписание, чтобы выполнить команду BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Создать резервную копию хронологии томов." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Удалите более старые версии резервных копий базы данных, которые больше не требуются.	Создайте расписание, чтобы выполнить команду DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Удалить старые резервные копии базы данных." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Удалите объекты, у которых превышен допустимый срок хранения.	Создайте расписание, чтобы выполнить команду EXPIRE INVENTORY. Задайте параметр RESOURCE на основе размера системы, которую вы конфигурируете, так чтобы он был равен числу ядер процессора, заданному вами для вашей системы. Например, введите следующую команду, чтобы создать расписание с именем EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Удалить проср. объекты." startdate=today starttime=14:00:00 duration=1 durunits=hours`

Операция	Примеры команд и дополнительная информация
Высвободите пространство.	Создайте расписание, чтобы выполнить команду RECLAIM STGPOOL. Например, введите следующую команду, чтобы создать расписание с именем RECLAIM: `define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours` Совет: Чтобы довести пропускную способность до максимума, можно задать число параллельных процессов, которые следует использовать для высвобождения пространства. Обновите пул хранения на ленте, используя команду UPDATE STGPOOL, и задайте значение для параметра RECLAIMPROCESS. Например, если у вас есть 12 ленточных накопителей, задайте `RECLAIMPROCESS=5`. Поскольку для каждого процесса высвобождения используются два накопителя, общее число накопителей, которые могут использоваться для восстановления, равно 10. Два накопителя зарезервированы для операций резервного копирования.

Дальнейшие действия

После того как вы создадите расписания задач по обслуживанию сервера, вы сможете увидеть их в компоненте Центр операций, выполнив следующие шаги:

1. В строке меню Центр операций установите указатель мыши на Серверы.
2. Щелкните по Обслуживание.

- Перемещение носителей резервных копий
  Для восстановления после аварии необходимы тома с резервными копиями базы данных, тома пулов хранения копий и дополнительные файлы. Чтобы быть готовым к аварийной ситуации, нужно выполнять ежедневные задачи.

Ссылки, связанные с данной:
UPDATE STGPOOL (обновить пул хранения)
DEFINE SCHEDULE (определение расписания выполнения административных команд)
Информация, связанная с данной:
DEFINE STGPOOL (определение тома в пуле хранения)

Определение расписаний клиентов

Используйте Центр операций, чтобы создавать расписания для операций клиентов.

Процедура

1. В строке меню Центр операций установите указатель мыши на Клиенты.
2. Щелкните по Расписания.
3. Щелкните по + Расписание.
4. Выполните шаги в мастере Создать расписание. Задайте запуск расписаний резервного копирования клиента в 22:00, основываясь на операциях по обслуживанию сервера, которые вы запланировали в разделе Как задать расписания для операций по обслуживанию сервера.

Подключение ленточных устройств к серверу

Прежде чем сервер сможет использовать накопитель на магнитной ленте, надо подключить это устройство к системе сервера и установить соответствующие драйверы ленточных устройств.

Об этой задаче

Чтобы оптимизировать производительность системы, используйте быстрые ленточные устройства с высокой мощностью. Предоставьте достаточно ленточных накопителей, чтобы их число удовлетворяло вашим бизнес-требованиям.

Подключите ленточные устройства на их собственном адаптере шины хоста (host bus adapter, HBA), не используемом совместно с другими типами устройств, например, дисководом.. Ленточные накопители IBM® предъявляют ряд особых требований к HBA и связанным драйверам.

-  Операционные системы AIX  Операционные системы LinuxПодключение устройства автоматизированной библиотеки к компьютеру
  Можно подключить устройство автоматизированной библиотеки к компьютеру для сохранения данных на ленте.
- Выбор драйвера ленточного устройства
  Чтобы использовать ленточные устройства с IBM Spectrum Protect, надо установить соответствующий драйвер ленточных устройств.
-  Операционные системы AIX  Операционные системы LinuxСпециальные имена файлов для ленточных устройств
  Серверу IBM Spectrum Protect требуется имя специального файла для ленточного устройства при работе с ленточными устройствами, сменными носителями и устройствами со съемными носителями.
- Установка и конфигурирование драйверов ленточных устройств
  Чтобы использовать ленточные устройства в сочетании с IBM Spectrum Protect, нужно установить соответствующий драйвер ленточных устройств.

Подключение устройства автоматизированной библиотеки к компьютеру

Можно подключить устройство автоматизированной библиотеки к компьютеру для сохранения данных на ленте.

Об этой задаче

Перед подключением устройства автоматизированной библиотеки ознакомьтесь со следующими ограничениями:

- Подключаемые устройства должны находиться на собственном адаптере шины хоста (Host Bus Adapter - HBA).
- Не используйте HBA совместно с другими типами устройств, такими как диски.
- В случае многопортовых адаптеров HBA Fibre Channel устройства должны подключаться к собственным портам. Эти порты не должны использоваться другими типами устройств.
- Ленточные накопители IBM® имеют ряд особых требований к HBA и соответствующим драйверам. Информацию об устройствах смотрите на веб-сайте для вашей операционной системы:
  - IBM Spectrum ProtectПоддерживаемые устройства для AIX
  - IBM Spectrum ProtectПоддерживаемые устройства для Linux и Windows

Процедура

Чтобы использовать адаптер Fibre Channel (FC), сделайте следующее:

1. Установите адаптер FC и связанные драйверы.
2. Установите необходимые драйверы для подключенных устройств смены носителей.

-  Операционные системы AIX  Операционные системы LinuxУстановка режима библиотеки
  Чтобы обеспечить серверу IBM Spectrum Protect доступ к библиотеке SCSI, нужно задать для ленточного устройства подходящий режим.

Понятия, связанные с данным:
Выбор драйвера ленточного устройства

Выбор драйвера ленточного устройства

Чтобы использовать ленточные устройства с IBM Spectrum Protect, надо установить соответствующий драйвер ленточных устройств.

- Драйверы ленточных устройств IBM
  Драйверы ленточных устройств IBM® доступны для большинства маркированных устройств IBM.

- Драйверы ленточных устройств IBM Spectrum Protect
  Сервер IBM Spectrum Protect предоставляет драйверы для работы с ленточными устройствами.

Ссылки, связанные с данной:
Установка и конфигурирование драйверов ленточных устройств

Драйверы ленточных устройств IBM

Драйверы ленточных устройств IBM® доступны для большинства маркированных устройств IBM.

Скачать драйверы ленточных устройств IBM можно с сайта Fix Central:

1. Перейдите на веб-сайт Fix Central: Веб-сайт Fix Central.
2. Щелкните по Выберите продукт.
3. Выберите Система хранения в меню Группа продуктов.
4. Выберите Ленточные системы в меню Система хранения.
5. Выберите Ленточные драйверы и программы в меню Ленточные системы.
6. Выберите Драйверы ленточных устройств в меню Ленточные драйверы и программы. В дополнение к ленточным драйверам вы также получаете доступ к инструментам, например, инструменту диагностики IBM Tape Diagnostic Tool (ITDT).
7. Выберите свою операционную систему в меню Платформа.

 Операционные системы AIX  Операционные системы Windows

Новейший список устройств и уровней операционных систем, поддерживаемых драйверами ленточных устройств IBM, смотрите на веб-сайте поддерживаемых устройств IBM Spectrum Protect по адресу: Поддерживаемые устройства для AIX и Windows.

 Операционные системы Linux

Новейший список ленточных устройств и уровней операционных систем, поддерживаемых драйверами ленточных устройств IBM, смотрите на веб-сайте поддерживаемых устройств IBM Spectrum Protect по адресу Поддерживаемые устройства для Linux.

Драйверы ленточных устройств IBM поддерживают только некоторые уровни ядра Linux. Информацию о поддерживаемых уровнях ядра смотрите а источнике Веб-сайт Fix Central.

Драйверы ленточных устройств IBM Spectrum Protect

Сервер IBM Spectrum Protect предоставляет драйверы для работы с ленточными устройствами.

Вместе с сервером устанавливается драйвер ленточных устройств IBM Spectrum Protect.

 Операционные системы AIX

Можно использовать универсальный драйвер ленточных накопителей SCSI, обеспеченный в операционной системе IBM® AIX для работы с накопителями на магнитной ленте, не поддерживаемыми драйвером устройств IBM Spectrum Protect. Если используется универсальный драйвер ленточных накопителей SCSI AIX, то класс устройства GENERICTAPE должен иметь значение типа устройства, определенный в команде DEFINE DEVCLASS.

В случае использования следующих ленточных устройств можно выбирать между установкой драйвера ленточных устройств IBM Spectrum Protect и собственного драйвера устройств операционной системы:

- ECART
- LTO (не от IBM)

Все SCSI-библиотеки, содержащие ленточные устройства из этого списка, должны использовать драйвер чейнджера IBM Spectrum Protect.

Драйверы ленточных устройств от других поставщиков оборудования могут использоваться, если они связаны с классом устройств GENERICTAPE. Универсальные драйверы устройств не поддерживаются в классах устройств WORM (write-one read-many).

 Операционные системы Linux

Можно использовать драйвер устройств Passthru IBM Spectrum Protect. Для драйверов устройств Passthru IBM Spectrum Protect требуется универсальный драйвер устройств Linux SCSI (sg) вместе с операционной системой Linux для установки ядер.

Например, можно установить драйвер устройств Passthru IBM Spectrum Protect для следующих ленточных устройств:

- ECART
- LTO (не от IBM)

Все библиотеки SCSI, содержащие накопители на магнитной ленте без метки IBM из указанного списка, должны использовать драйвер устройств Passthru IBM Spectrum Protect.

Использовать универсальный драйвер устройств ленточных накопителей SCSI (st), предоставляемый операционной системой Linux, нельзя. Поэтому тип устройств GENERICTAPE не поддерживается для команды DEFINE DEVCLASS.

 Операционные системы WindowsВместо драйвера устройств IBM Spectrum Protect можно выбрать собственный драйвер устройств, сертифицированный в Windows Hardware Qualification Lab. Лаборатория Windows Hardware Qualification Lab сертифицировала собственный драйвер устройств как драйвер, который можно использовать только для устройств с меткой не IBM и для ленточных накопителей не IBM. Для собственного драйвера устройства, сертифицированного лабораторией Windows Hardware Qualification Lab, можно выбрать либо драйвер устройств passthru SCSI IBM Spectrum Protect, либо собственный драйвер ленточных устройств Windows. Если используется SCSI-драйвер устройства passthru, то класс устройства в команде DEFINE DEVCLASS не может быть GENERICTAPE. Если используется собственный драйвер устройств, классом устройств должно быть GENERICTAPE.

Специальные имена файлов для ленточных устройств

Серверу IBM Spectrum Protect требуется имя специального файла для ленточного устройства при работе с ленточными устройствами, сменными носителями и устройствами со съемными носителями.

 Операционные системы AIX
В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Табл. 1 указано имя устройства, также называющееся имя специального файла, соответствующее накопителю или библиотеке. Для получения имени специального файла устройства можно воспользоваться командой операционной системы SMIT. В примерах *x* задает целое число, 0 или больше.

Табл. 1. Примеры устройств

Устройство	**Пример устройства**	**Логическое имя файла**
Ленточные накопители, поддерживаемые драйвером устройств IBM Spectrum Protect	/dev/mt*x*	mt*x*
Ленточные накопители, поддерживаемые драйвером ленточных устройств IBM	/dev/rmt*x*	rmt*x*
Ленточные накопители, поддерживаемые универсальным драйвером ленточных устройств AIX IBM	/dev/rmt*x*	rmt*x*
Устройства библиотеки, поддерживаемые драйвером устройств IBM Spectrum Protect	/dev/lb*x*	lb*x*
Устройства библиотеки, поддерживаемые драйвером ленточных устройств IBM	/dev/smc*x*	smc*x*

 Операционные системы Linux
В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Табл. 2 указано имя устройства (другое имя - имя специального файла), соответствующее накопителю или библиотеке. В примерах *x* задает целое число, 0 или больше.

Табл. 2. Примеры устройств

Устройство	**Пример устройства**	**Логическое имя файла**
Ленточные накопители, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	/dev/tsmscsi/mt*x*	mt*x*
Ленточные накопители, поддерживаемые драйвером устройств lin_tape IBM	/dev/IBMtape*x*	IBMtape*x*

Устройство	Пример устройства	Логическое имя файла
Устройства библиотеки, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	/dev/tsmscsi/lb*x*	lb*x*
Устройства библиотеки, поддерживаемые драйвером устройств lin_tape IBM	/dev/IBMchanger*x*	IBMchanger*x*

Операционные системы Windows

В случае успешного конфигурирования устройства возвращается логическое имя файла. В таблице Табл. 3 указано имя устройства (другое имя - имя специального файла), соответствующее накопителю или библиотеке. В примерах *a*, *b*, *c*, *d* и *x* задают целое число, 0 или больше, где:

- *a* - ID назначения.
- *b* - LUN.
- *c* ID шины SCSI.
- *d* ID порта.

Табл. 3. Примеры устройств

Устройство	Пример устройства	Преобразованное имя устройства
Ленточные накопители, поддерживаемые драйвером устройств IBM Spectrum Protect	mt*a.b.c.d*	mt*a.b.c.d*
Ленточные накопители, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	mt*a.b.c.d*	mt*a.b.c.d*
Ленточные накопители, поддерживаемые драйвером устройств IBM	Tape*x*	mt*a.b.c.d*
Устройства библиотек, поддерживаемые драйвером устройств IBM Spectrum Protect	lb.*a.b.c.d*	lb*a.b.c.d*
Устройства библиотек, поддерживаемые драйвером устройств Passthru IBM Spectrum Protect	lb*a.b.c.d*	lb*a.b.c.d*
Устройства библиотек, поддерживаемые драйвером устройств IBM	Changer*x*	lb*a.b.c.d*

Установка и конфигурирование драйверов ленточных устройств

Чтобы использовать ленточные устройства в сочетании с IBM Spectrum Protect, нужно установить соответствующий драйвер ленточных устройств.

IBM Spectrum Protect поддерживает все устройства, которые поддерживаются драйверами ленточных устройств IBM®. Однако IBM Spectrum Protect поддерживает не все уровни операционных систем, поддерживаемые драйверами ленточных устройств IBM.

- Установка и конфигурирование драйверов устройств IBM для ленточных устройств IBM
  Установите и сконфигурируйте драйвер ленточных устройств IBM для использования ленточного устройства IBM.
- Операционные системы AIXКонфигурирование драйверов ленточных устройств в системах AIX
  Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы ленточных устройств не IBM в системах AIX.
- Операционные системы LinuxКонфигурирование драйверов ленточных устройств в системах Linux
  В следующих разделах описаны установка и конфигурирование драйверов ленточных устройств в Linux.
- Операционные системы WindowsКонфигурирование драйверов ленточных устройств в системах Windows
  Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы для ленточных устройств и библиотек в системах Windows.

Установка и конфигурирование драйверов устройств IBM для ленточных устройств IBM

Установите и сконфигурируйте драйвер ленточных устройств IBM® для использования ленточного устройства IBM.

Об этой задаче

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в публикации *Драйверы ленточных устройств IBM: Руководство по установке и использованию*.

 Операционные системы AIXПосле завершения процедуры установки в соответствии с *IBM Tape Device Drivers Installation and User's Guide (Руководство по установке и использованию драйверов накопителей на магнитной ленте IBM)* могут появиться различные сообщения, зависящие от устанавливаемого драйвера устройств. При установке драйвера для ленточного устройства IBM или библиотеки выдаются следующие сообщения:

```
rmtx Available
```

или

```
smcx Available
```

Обратите внимание на значение x, которое назначено драйвером ленточных устройств IBM. Чтобы определить имя специального файла устройства, введите одну из следующих команд:

- Для ленточных накопителей: `ls -l /dev/rmt*`
- Для ленточных библиотек: `ls -l /dev/smc*`

Имя файла может оканчиваться дополнительными символами, указывающими на различные характеристики устройств. Эти символы не требуются для IBM Spectrum Protect. Для драйверов устройств IBM в параметре DEVICE команды DEFINE PATH используется базовое имя файла для связывания устройства с накопителем (/dev/rmtx) или с библиотекой (/dev/smcx).
После установки драйвера устройства можно использовать System Management Interface Tool (SMIT), чтобы сконфигурировать ленточные накопители и ленточные библиотеки не IBM. Сделайте следующее:

1. Запустите программу интерфейса системного управления (SMIT).
2. Щелкните по Устройства.
3. Выберите Устройства IBM Spectrum Protect.
4. Выберите Устройства, подключенные к SAN Fibre Channel.
5. Выберите команду Обнаружить устройства, поддерживаемые IBM Spectrum Protect. Дождитесь завершения процесса обнаружения.
6. Вернитесь в меню Устройства, подключенные к SAN Fibre Channel и щелкните по Список атрибутов обнаруженного устройства.

 Операционные системы LinuxПосле завершения процедуры установки в соответствии с *IBM Tape Device Drivers Installation and User's Guide (Руководство по установке и использованию драйверов накопителей на магнитной ленте IBM)* могут появиться различные сообщения, зависящие от устанавливаемого драйвера устройств. При установке драйвера устройств для устройства IBM LTO или 3592 будут возвращены следующие сообщения:

```
IBMtapex Available
```

или

```
IBMChangerx Available
```

Обратите внимание на значение x, которое назначено драйвером ленточных устройств IBM. Чтобы определить имя специального файла устройства, введите одну из следующих команд:

- Для ленточных накопителей: `ls -l /dev/IBMtape*`
- Для ленточных библиотек: `ls -l /dev/IBMChange*`

Имя файла может оканчиваться дополнительными символами, указывающими на различные характеристики устройств. Эти символы не требуются для IBM Spectrum Protect. Для драйверов устройств IBM в параметре DEVICE команды DEFINE PATH используется базовое имя файла для связывания устройства с накопителем (/dev/IBMtapex) или с библиотекой (/dev/IBMChangerx).
Ограничение: Тип устройства этого класса не должен быть GENERICTAPE.
 Операционные системы WindowsВ операционных системах Windows к IBM Spectrum Protect прилагается два драйвера устройств:

Драйвер устройств Passthru
: Если производитель ленточного устройства предоставляет драйвер устройств SCSI, установите драйвер устройств passthru IBM Spectrum Protect.

Драйвер устройства SCSI для ленточных устройств
: Если производитель ленточного устройства не предоставляет драйвер устройств SCSI, установите драйвер устройств SCSI IBM Spectrum Protect для ленточных устройств. Имя файла драйвера - tsmscsi64.sys.

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в публикации *IBM Tape Device Drivers Installation and User's Guide* (Руководство по установке и использованию драйверов ленточных устройств IBM). После установки драйвера ленточных устройств IBM сервер задает имя специального файла, Tape*X*, для ленточных устройств IBM или имя Changer*Y* для устройств со сменными носителями IBM. В случае драйвера устройств SCSI IBM Spectrum Protect или драйвера устройств passthru IBM Spectrum Protect можно ввести команду операционной системы Windows, regedit, чтобы проверять имя специального файла устройства и драйвер. На сервере IBM Spectrum Protect также есть утилита для проверки устройства для операционной системы Windows. Утилита tsmdlst включена в пакет сервера. Чтобы использовать утилиту, выполните следующие шаги:

1. Убедитесь, что установлен интерфейс прикладного программирования (API) адаптера шины хоста.
2. Для получения информации об устройстве из хост-системы введите:

   ```
   tsmdlst
   ```

- Операционные системы AIXОперационные системы LinuxДоступ к многонаправленому вводу-выводу на ленточных устройствах IBM
  Многонаправленный ввод-вывод - это метод, в котором для доступа к одному и тому же физическому устройству используются разные пути, например, через несколько адаптеров шины хоста (host bus adapter, HBA) или коммутаторов. Использование многонаправленной технологии позволяет гарантировать, что не возникнет единая точка сбоев.

Понятия, связанные с данным:
Доступ к многонаправленому вводу-выводу на ленточных устройствах IBM
Операционные системы AIX

Конфигурирование драйверов ленточных устройств в системах AIX

Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы ленточных устройств не IBM® в системах AIX.

Об этой задаче

Инструкции по установке и конфигурированию драйверов ленточных устройств IBM смотрите в публикации *Драйверы ленточных устройств IBM: Руководство по установке и использованию*.

- Операционные системы AIXУстройства SCSI и устройства, подключаемые по оптоволоконным каналам
  Меню и подсказки для созданий определений устройств IBM Spectrum Protect в SMIT позволяют управлять устройствами SCSI и устройствами, подключаемыми по оптоволоконным каналам (Fibre Channel, FC).
- Операционные системы AIXКонфигурирование драйверов устройств IBM Spectrum Protect для авточейнджеров
  Используйте описанную процедуру, чтобы сконфигурировать драйверы устройств IBM Spectrum Protect для авточейнджеров в библиотеках не-IBM.
- Операционные системы AIXКонфигурирование драйверов устройств IBM Spectrum Protect для ленточных накопителей
  Используйте следующую процедуру для конфигурирования драйверов устройств IBM Spectrum Protect для авточейнджеров в библиотеках, приобретенных у других поставщиков.
- Операционные системы AIXКонфигурирование устройств, подключенных к SAN Fibre Channel
  Чтобы сконфигурировать устройство, подключенное к SAN Fibre Channel, сделайте следующее.

Операционные системы AIX

Устройства SCSI и устройства, подключаемые по оптоволоконным каналам

Меню и подсказки для созданий определений устройств IBM Spectrum Protect в SMIT позволяют управлять устройствами SCSI и устройствами, подключаемыми по оптоволоконным каналам (Fibre Channel, FC).

Главное меню для IBM Spectrum Protect содержит два пункта:

Устройства с интерфейсом SCSI
: Этот вариант используется для конфигурирования устройств SCSI, подключенных к адаптеру SCSI на компьютере хоста.

Устройства sAN с подключением по интерфейсу fibre channel

Этот вариант используется для конфигурирования устройств, подключенных к адаптеру FC на хосте. Выберите один из следующих атрибутов:

Показать атрибуты обнаруженного устройства
: Служит для вывода списка атрибутов устройства, зарегистрированного в текущей базе данных ODM.

  - ID порта FC:

    ID 24-битного порта FC (N(L)_порт или F(L)_порт). Это идентификатор адреса, имеющий уникальное значение в пределах сети, к которой подключено устройство. В среде с коммутатором или коммутирующей матрицей этот параметр может определяться коммутатором, при этом 2 верхних байта не равны нулю. В среде Private Arbitrated Loop в качестве значения этого параметра используется физический адрес управляемой петли (AL_PA), при этом 2 верхних байта равны нулю. Чтобы определить, каким образом назначается AL_PA или ID порта, обратитесь к производителям оборудования FC.

  - Сопоставленный ID LUN:

    Устройство моста FC-SCSI (которое называется также конвертером, маршрутизатором или шлюзом). Сведения о сопоставлении LUN можно получить у производителей мостов. Не следует изменять значения ID, отображенных на LUN.

  - Глобальное имя (wildwide name):

    Глобальное имя порта, к которому подключено устройство. Это уникальный 64-разрядный идентификатор, присваиваемый производителями компонентов FC, например, мостов, или собственных устройств FC. Обратитесь к вашим поставщикам FC, чтобы узнать глобальное имя порта.

  - ID продукта:

    ID продукта для устройства. Для определения идентификатора продукта обратитесь к производителям устройств.

Обнаружение устройств, поддерживаемых IBM Spectrum Protect
: Эта опция служит для обнаружения устройств, поддерживаемых IBM Spectrum Protect, в сети хранения данных FC, и присвоения им состояния Доступно. При добавлении устройства в существующую среду SAN или при удалении устройства из среды необходимо повторно выполнить обнаружение устройств с помощью этой опции. Чтобы текущие значения атрибутов устройств отображались при выборе опции Список атрибутов обнаруженного устройства, необходимо сначала обнаружить устройства. Поддерживаемыми устройствами в сети хранения данных FC могут быть ленточные накопители и авточейнджеры. Драйвер устройств IBM Spectrum Protect игнорирует устройства всех других типов, например, жесткие диски.

Удаление всех определенных устройств
: Эта опция служит для удаления из IBM Spectrum Protect всех устройств, подключенных к сети хранения данных FC, для которых указано состояние `DEFINED` в базе данных ODM. После удаления всех определенных устройств при необходимости можно повторно запустить процесс обнаружения устройств с помощью опции `Обнаружить устройства, поддерживаемые IBM Spectrum Protect`.

Удалить устройство
: Эта опция служит для удаления из IBM Spectrum Protect одного устройства, подключенного к сети хранения данных FC, для которого указано состояние `DEFINED` в базе данных ODM. После удаления этого устройства при необходимости можно повторно выполнить его обнаружение с помощью опции `Обнаружить устройства, поддерживаемые IBM Spectrum Protect`.

Операционные системы AIX

Конфигурирование драйверов устройств IBM Spectrum Protect для авточейнджеров

Используйте описанную процедуру, чтобы сконфигурировать драйверы устройств IBM Spectrum Protect для авточейнджеров в библиотеках не-IBM.

Процедура

Запустите программу интерфейса системного управления (SMIT), чтобы сконфигурировать драйвер устройства для каждого авточейнджера или роботизированного устройства.

1. Выберите элемент Устройства.
2. Выберите элемент IBM Spectrum ProtectУстройства.
3. Выберите элемент Библиотека/устройство смены носителей.
4. Выберите команду Добавить библиотеку/устройство смены носителей.
5. Выберите IBM Spectrum Protect-SCSI-LB для всех библиотек, поддерживаемых IBM Spectrum Protect.
6. Выберите адаптер, к которому подключается устройство. Это число приводится в формате 00-0X, где X – это номер слота, в который установлена плата адаптера SCSI.
7. При появлении приглашения введите адрес устанавливаемого устройства для параметра CONNECTION. Адрес подключения выражается двузначным числом. Первая цифра – это идентификатор SCSI (значение, записанное в таблице). Вторая цифра – номер логического устройства SCSI (LUN), который обычно равняется нулю, если не указано иное. Идентификатор SCSI и номер LUN разделяются запятой (,). Например, в адресе подключения `4,0` используются идентификатор SCSI=4 и LUN=0.
8. Щелкните по ВЫПОЛНИТЬ.

   Откроется сообщение (логическое имя файла) вида `lbX Available`. Запишите числовое значение X, автоматически назначаемое системой. Используйте эти сведения для заполнения поля Имя устройства в контрольном списке.

   Например, если появится сообщение `lb0 Available`, то поле Имя устройства в контрольном списке должно содержать /dev/lb0. Всегда используйте префикс /dev/ перед именем, указанным программой SMIT.

 Операционные системы AIX

Конфигурирование драйверов устройств IBM Spectrum Protect для ленточных накопителей

Используйте следующую процедуру для конфигурирования драйверов устройств IBM Spectrum Protect для авточейнджеров в библиотеках, приобретенных у других поставщиков.

Процедура

Важное замечание: IBM Spectrum Protect не может перезаписывать магнитные ленты *tar* или *dd*, однако программы *tar* и *dd* могут перезаписывать магнитные ленты IBM Spectrum Protect.
Ограничение: Совместное использование ленточных накопителей возможно только в случае, если накопитель не определен или сервер не запущен. Команда MKSYSB не действует, если IBM Spectrum Protect и AIX совместно используют один и тот же накопитель или несколько накопителей. Чтобы использовать в сочетании с устройством SCSI собственный драйвер операционной системы для ленточных устройств, устройство нужно сначала сконфигурировать в AIX, а затем в IBM Spectrum Protect. Сведения о собственных драйверах устройств смотрите в документации AIX.

Запустите программу интерфейса системного управления (SMIT), чтобы сконфигурировать драйвер устройства для каждого накопителя (в том числе для накопителей, входящих в состав библиотек).

1. Выберите элемент Устройства.
2. Выберите элемент IBM Spectrum ProtectУстройства.
3. Выберите элемент Ленточный носитель.
4. Выберите элемент Добавить ленточный носитель.
5. Выберите IBM Spectrum Protect-SCSI-MT для любого поддерживаемого ленточного накопителя.
6. Выберите адаптер, к которому подключается устройство. Это число приводится в формате 00-0X, где X - это номер слота, в который установлена плата адаптера SCSI.
7. При появлении приглашения введите адрес устанавливаемого устройства для параметра CONNECTION. Адрес подключения выражается двузначным числом. Первая цифра - это идентификатор SCSI (значение, записанное в таблице). Вторая цифра - номер логического устройства SCSI (LUN), который обычно равняется нулю, если не указано иное. Идентификатор SCSI и номер LUN разделяются запятой (,). Например, в адресе подключения `4,0` используются идентификатор SCSI=4 и LUN=0.
8. Щелкните по ВЫПОЛНИТЬ. Появится сообщение:

   При конфигурировании драйвера для ленточного устройства (отличного от ленточного накопителя IBM®) появится сообщение (логическое имя файла) в формате `mtX Available`. Запишите числовое значение X, автоматически назначаемое системой. Используйте эти сведения для заполнения поля Имя устройства в контрольном списке.

Например, если появится сообщение `mt0 Available`, то поле Имя устройства в контрольном списке должно содержать /dev/mt0. Всегда используйте префикс /dev/ перед именем, указанным программой SMIT.

Операционные системы AIX

Конфигурирование устройств, подключенных к SAN Fibre Channel

Чтобы сконфигурировать устройство, подключенное к SAN Fibre Channel, сделайте следующее.

Процедура

1. Запустите программу интерфейса системного управления (SMIT).
2. Выберите элемент Устройства.
3. Выберите элемент IBM Spectrum ProtectУстройства.
4. Выберите элемент Устройства, подключенные к SAN Fibre Channel.
5. Выберите Обнаружить устройства, поддерживаемые IBM Spectrum Protect. Процесс обнаружения может занять некоторое время.
6. Вернитесь в меню Fibre Channel и выберите Список атрибутов обнаруженного устройства.
7. Обратите внимание на 3-символьный идентификатор устройства, который используется при определении пути к устройству в IBM Spectrum Protect. Например, если ленточный накопитель имеет идентификатор `mt2`, то укажите /dev/mt2 в качестве имени устройства.

Операционные системы Linux

Конфигурирование драйверов ленточных устройств в системах Linux

В следующих разделах описаны установка и конфигурирование драйверов ленточных устройств в Linux.

- Операционные системы LinuxКонфигурирование промежуточных (Passthru) драйверов IBM Spectrum Protect для ленточных накопителей и библиотек
  Чтобы использовать драйвер IBM Spectrum Protect Linux Passthru, нужно выполнить описанные ниже действия.
- Операционные системы LinuxУстановка драйверов устройств адаптера zSeries Linux Fibre Channel (zfcp)
  Драйвер устройств оптоволоконного адаптера zSeries Linux Fibre Channel (zfcp) - это специальный драйвер адаптера для системы IBM® zSeries.
- Операционные системы LinuxИнформация об устройствах SCSI в системе
  Информация об устройствах, которые видны вашей системе, находится в файле */proc/scsi/scsi.* Этот файл содержит список всех обнаруженных устройств SCSI.
- Операционные системы LinuxПредотвращение перезаписи меток магнитных лент
  Драйвер устройств Passthru IBM Spectrum Protect использует универсальный драйвер устройств SCSI Linux (sg) для управления ленточными устройствами, подключенным к системе. Если универсальный драйвер ленточного устройства SCSI Linux (st) загружен в ядро и конфигурирует подключенные ленточные устройства, могут возникнуть конфликты управления устройствами, так как универсальный драйвер sg и драйвер st могут пытаться контролировать одно и то же устройство.

Операционные системы Linux

Конфигурирование промежуточных (Passthru) драйверов IBM Spectrum Protect для ленточных накопителей и библиотек

Чтобы использовать драйвер IBM Spectrum Protect Linux Passthru, нужно выполнить описанные ниже действия.

Процедура

1. Убедитесь, что устройство подключено к системе, включено и активно.
2. Убедитесь, что устройство правильно определено системой, с помощью следующей команды:

```
cat /proc/scsi/scsi
```

3. Убедитесь, что у вас установлен пакет драйвера устройств IBM Spectrum Protect (tsmscsi) и пакет сервера хранения.
4. В пакете драйвера устройств IBM Spectrum Protect существует два метода конфигурирования драйверов: autoconf и tsmscsi. При использовании любого из этих способов выполняются следующие задачи.
   - Загрузка универсального драйвера SCSI операционной системы Linux (sg) в ядро.
   - Создание необходимых специальных файлов для драйвера Passthru.
   - Создание файлов сведений об устройствах для ленточных устройств (/dev/tsmscsi/mtinfo) и библиотек (/dev/tsmscsi/lbinfo).
5. Запустите предпочтительный для вас метод конфигурирования (autoconf или tsmscsi) для драйвера IBM Spectrum Protect Passthru.
   - Чтобы выполнить конфигурирование с помощью autoconf, введите следующую команду:

     ```
     autoconf
     ```

   - Чтобы осуществить конфигурирование с помощью tsmscsi, выполните следующие действия:
     a. Скопируйте примеры файлов конфигурации, находящиеся в каталоге установки, из *mt.conf.smp* и *lb.conf.smp* в *mt.conf* и *lb.conf*, соответственно.
     b. Отредактируйте файлы mt.conf и lb.conf. Добавьте один раздел (как показано в примере в начале файла) для каждого сочетания конечного объекта, идентификатора и номера логического устройства SCSI. Каждое сочетание записей о конечном объекте, идентификаторе и номере логического устройства SCSI соответствует ленточному накопителю или библиотеке, которые требуется сконфигурировать. Убедитесь, что файлы соответствуют следующим требованиям.
        - Удалите пример, расположенный в начале файлов.
        - Каждый раздел должен начинаться с новой строки.
        - После последнего раздела должна начинаться новая строка.
        - Ни в одном из файлов не должно быть символа решетки (#).
     c. Запустите сценарий tsmscsi из каталога установки драйвера устройств.
6. Проверьте правильность конфигурирования устройства, просмотрев текстовые файлы для ленточных устройств (/dev/tsmscsi/mtinfo) и библиотек (/dev/tsmscsi/lbinfo).
7. Определите имена специальных файлов для ленточных накопителей и библиотек
   - Чтобы определить имена файлов для ленточных устройств, введите следующую команду:

     ```
     > ls  /dev/tsmscsi/mt*
     ```

   - Чтобы определить имена файлов для библиотек, введите следующую команду:

     ```
     > ls  /dev/tsmscsi/lb*
     ```

   Эти сведения помогают определить, какое из имен специальных файлов /dev/tsmscsi/mtx и /dev/tsmscsi/lbx необходимо указать для сервера при вводе команды DEFINE PATH.

Дальнейшие действия

При перезапуске хост-системы вы должны заново запустить сценарий autoconf или tsmscsi, чтобы переконфигурировать устройства IBM Spectrum Protect. Если вы перезапустите экземпляр сервера IBM Spectrum Protect, вам не нужно переконфигурировать устройства. Как правило, универсальный драйвер SCSI операционной системы Linux предварительно установлен в ядро. Чтобы убедиться, что драйвер загружен в ядро, введите следующую команду:

```
> lsmod | grep sg
```

Если драйвер не загружен в ядро, то введите команду modprobe sg, чтобы загрузить драйвер sg в ядро.
Операционные системы Linux

Установка драйверов устройств адаптера zSeries Linux Fibre Channel (zfcp)

Драйвер устройств оптоволоконного адаптера zSeries Linux Fibre Channel (zfcp) - это специальный драйвер адаптера для системы IBM® zSeries.

Об этой задаче

Дрвйверы ленточных устройств IBM Spectrum Protect и IBM могут работать на платформах zSeries с операционными системами Linux в 64-разрядных средах и поддерживают большую часть ленточных устройств независимых производителей оборудования (OEM) и IBM с оптоволоконными интерфейсами (Fibre Channel).

Дополнительные сведения о драйвере zfcp смотрите в публикации IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol* (Начинаем работу с протоколом zSeries Fibre Channel), которая находится по адресу: IBM Redbooks.

Процедура

1. Загрузите модуль qdio.
2. Установите драйвер zfcp.
3. Отобразите протокол Fibre Channel (FCP) и сконфигурируйте драйвер zfcp.
4. Установите и сконфигурируйте драйвер ленточного устройства IBM.

Операционные системы Linux

Информация об устройствах SCSI в системе

Информация об устройствах, которые видны вашей системе, находится в файле */proc/scsi/scsi*. Этот файл содержит список всех обнаруженных устройств SCSI.

Представлена следующая информация об устройствах: номер хоста, номер канала, ID SCSI, номер логического устройства, поставщик, уровень программно-аппаратного обеспечения, тип устройства и режим SCSI. Например, если в системе существуют библиотеки StorageTek и IBM®, шлюз SAN и несколько накопителей Quantum DLT, то файл */proc/scsi/scsi* будет выглядеть следующим образом:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor:  STK    Model: 9738     Rev: 2003
  Type:  Medium Changer         ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  PATHLIGHT Model: SAN Gateway     Rev: 32aC
  Type: Unknown         ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  QUANTUM  Model: DLT7000     Rev: 2560
  Type:  Sequential-Access         ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM     Model: 7337     Rev: 1.63
  Type:  Medium Changer         ANSI SCSI revision: 02
```

Операционные системы Linux

Предотвращение перезаписи меток магнитных лент

Драйвер устройств Passthru IBM Spectrum Protect использует универсальный драйвер устройств SCSI Linux (sg) для управления ленточными устройствами, подключенным к системе. Если универсальный драйвер ленточного устройства SCSI Linux (st) загружен в ядро и конфигурирует подключенные ленточные устройства, могут возникнуть конфликты управления устройствами, так как универсальный драйвер sg и драйвер st могут пытаться контролировать одно и то же устройство.

Об этой задаче

Если драйвер драйвер st управляет устройствами, которые использует IBM Spectrum Protect, внутренние метки лент IBM Spectrum Protect могут быть перезаписаны, и данные окажутся утерянными. Если программа использует драйвер st для управления устройствами и опция пропуска перемотки не задана, ленты автоматически перематываются после завершения операции. В ходе операции автоматической перемотки позиция ленты устанавливается в начальное положение. Если лента остается загруженной в накопитель, при следующей операции записи вне IBM Spectrum Protect метка магнитной ленты IBM Spectrum Protect перезаписывается, поскольку эта метка находится в начале ленты.

Чтобы предотвратить перезапись меток IBM Spectrum Protect, которая может привести к потере данных, убедитесь, что устройствами, используемыми IBM Spectrum Protect, управляет только драйвер Passthru IBM Spectrum Protect. Удалите драйвер st из ядра, или, если этот драйвер используют какие-либо программы в системе, удалите специальные файлы, соответствующие устройствам IBM Spectrum Protect.

Если для управления устройствами в вашей системе используется драйвер ленточных устройств IBM, то вы можете столкнуться с аналогичными проблемами при конфликте управления драйверов устройств. Посмотрите в документации к ленточным устройствам IBM, как устранить эту проблемы и предотвратить потерю данных.

Удалите драйвер st

Если другие программы в системе не используют устройства st, удалите драйвер st из ядра. Чтобы выгрузить драйвер st, введите следующую команду:

```
rmmod st
```

Удалите специальные файлы, соответствующие устройствам IBM Spectrum Protect

Если существуют программы, для которых требуется использование драйвера st, можно удалить специальные файлы, соответствующие устройствам IBM Spectrum Protect. Эти специальные файлы создаются драйвером st. После удаления этих файлов драйвер st больше не сможет управлять соответствующими устройствами IBM Spectrum Protect. Специальные файлы для ленточных устройств находятся в каталоге /dev/. Формат имен: /dev/[n]st[0-1024][l][m][a].

Выведите список имен специальных файлов устройств st и список имен специальных файлов устройств IBM Spectrum Protect при помощи команды ls. На основе выведенных последовательностей устройств можно найти в списке st устройства, соответствующие устройствам в списке IBM Spectrum Protect. Удалить устройства st можно при помощи команды rm.

Введите следующие команды, чтобы вывести список устройств st и IBM Spectrum Protect:

```
ls -l /dev/*st*
ls -l /dev/tsmscsi/mt*
```

Удалите устройства st при помощи команды `rm`:

```
rm /dev/*st*
```

Операционные системы Windows

Конфигурирование драйверов ленточных устройств в системах Windows

Ознакомьтесь с инструкциями, чтобы установить и сконфигурировать драйверы для ленточных устройств и библиотек в системах Windows.

- Операционные системы WindowsПодготовка к использованию драйвера passthru IBM Spectrum Protect для ленточных устройств и библиотек
  Чтобы использовать драйвер устройств passthru IBM Spectrum Protect Windows для ленточных накопителей и библиотек, надо установить драйвер и получить имена устройств, которые будет использовать сервер.
- Операционные системы WindowsКонфигурирование драйвера SCSI IBM Spectrum Protect для ленточных устройств и библиотек
  Если производитель ленточного накопителя или ленточной библиотеки не предоставляет драйвер устройств SCSI, вы должны установить драйвер устройств SCSI IBM Spectrum Protect.

Операционные системы Windows

Подготовка к использованию драйвера passthru IBM Spectrum Protect для ленточных устройств и библиотек

Чтобы использовать драйвер устройств passthru IBM Spectrum Protect Windows для ленточных накопителей и библиотек, надо установить драйвер и получить имена устройств, которые будет использовать сервер.

Прежде чем начать

1. Определите, поставляет ли производитель ленточного устройства или ленточной библиотеки драйвер устройств.
2. Если производитель предоставляет пакет драйверов устройств, скачайте пакет и установите его.
3. Сконфигурируйте драйвер устройств SCSI, следуя инструкциям производителя.

Процедура

1. Установите драйвер устройств passthru IBM Spectrum Protect.
2. Получите имена устройств, которые сервер должен использовать, выполнив одно из следующих действий:

- Введите на сервере команду QUERY SAN. В выходной информации будут показаны все имена устройств и связанные с ними серийные номера устройств.
- В каталоге сервера запустите утилиту tsmdlst.exe. В выходной информации будут показаны все имена устройств, связанные с ними серийные номера и связанные расположения устройств.
- В системной командной строке Windows введите команду regedit. Найдите в выходной информации имена файлов устройств на основе расположения устройств. Расположение состоит из ID порта, ID шины SCSI, ID LUN и ID объекта назначения SCSI. Формат имени файла устройства IBM Spectrum Protect - mt*A*.*B*.*C*.*C* для ленточных накопителей и lb*A*.*B*.*C*.*D* для ленточных библиотек, где:
  - *A* - ID назначения SCSI.
  - *B* - ID LUN.
  - *C* - ID шины SCSI.
  - *D* - ID порта.

 Операционные системы Windows

Конфигурирование драйвера SCSI IBM Spectrum Protect для ленточных устройств и библиотек

Если производитель ленточного накопителя или ленточной библиотеки не предоставляет драйвер устройств SCSI, вы должны установить драйвер устройств SCSI IBM Spectrum Protect.

Об этой задаче

Имя файла драйвера устройств SCSI IBM Spectrum Protect - tsmscsi64.sys.

Процедура

1. Найдите устройство на консоли менеджера устройств (devmgmt.msc) и выберите его. Ленточные накопители перечислены в разделе Ленточные накопители, а чейнджеры носителей - в разделе Чейнджеры носителей.
2. Сконфигурируйте устройство для использования драйвера устройств tsmscsi64.sys:
   a. Щелкните правой кнопкой мыши по устройству и щелкните по Обновить программу драйвера.
   b. Щелкните по Обзор моего компьютера для поиска программы драйвера.
3. Щелкните по Разрешить мне выбрать из списка драйверов устройств на моем компьютере.
4. Щелкните по Далее.
5. Выберите соответствующую опцию:
   a. В случае ленточного накопителя выберите IBM Spectrum Protect for Tape Drives.
   b. В случае устройства со сменой носителей выберите IBM Spectrum Protect for Medium Changers.
6. Щелкните по Далее.
7. Щелкните по Закрыть.
8. Убедитесь, что устройство сконфигурировано правильно для драйвера устройств tsmscsi64.
   a. Щелкните правой кнопкой мыши по устройству и щелкните по Свойства.
   b. Щелкните по вкладке Драйвер и выберите Сведения о драйвере. В окне Сведения о драйвере будет показан драйвер устройств, управляющий устройством.

Конфигурирование библиотек для использования сервером

Чтобы использовать библиотеки для системы хранения одного сервера IBM Spectrum Protect, необходимо сначала сконфигурировать устройства в системе этого сервера.

Прежде чем начать

1. Подключите устройства к серверу. Следуйте инструкциям в Подключение устройства автоматизированной библиотеки к компьютеру.
2. Выберите накопители на ленточных устройствах. Следуйте инструкциям в Выбор драйвера ленточного устройства.
3. Установите и сконфигурируйте драйверы ленточных устройств. Следуйте инструкциям в Установка и конфигурирование драйверов ленточных устройств.
4. Задайте имена устройств, необходимые для определения библиотеки на сервере. Следуйте инструкциям в Специальные имена файлов для ленточных устройств.

Процедура

1. Задайте библиотеку и путь с сервера до библиотеки. Следуйте инструкциям в Определение библиотек.
2. Определите накопители в библиотеке. Следуйте инструкциям в Определение носителей.

   Для библиотек SCSI можно использовать команду PERFORM LIBACTION, чтобы задать накопители и пути для библиотеки в один шаг, вместо выполнения двух шагов: 2 и 3. Чтобы использовать команду PERFORM LIBACTION для назначения накопителей и путей для библиотеки, нужно, чтобы поддерживалась и была включена опция SANDISCOVERY.

3. Задайте путь с сервера к каждому накопителю, используя команду DEFINE PATH.
4. Задайте класс устройств. Следуйте инструкциям в Описание классов ленточных устройств.

   Классы устройств задают форматы записи для накопителей и классифицируют их по типу. Используйте значение по умолчанию FORMAT=DRIVE как формат записи только в том случае, если все накопители, связанные с данным классом устройств, могут читать все носители и производить на них запись.

   Например, у вас есть смесь накопителей Ultrium поколения 3 и Ultrium поколения 4, но у вас есть только носитель Ultrium поколения 3. Вы можете задать FORMAT=DRIVE, так как накопители поколения 4 и поколения 3 могут читать носители поколения 3 и производить на них запись.
5. Задайте пул хранения при помощи команды DEFINE STGPOOL.
   Рассмотрите следующие основные варианты для определения пулов хранения:
   - Чистые тома, представляющие собой пустые тома, доступные для использования. Если вы зададите максимальное число чистых томов в пуле хранения, сервер сможет выбрать тома из чистых томов, имеющихся в библиотеке.

     Если использование чистых томов запрещено, необходимо выполнить дополнительные действия, чтобы явно определить каждый том, который будет использоваться в пуле хранения. Кроме этого, задайте параметр MAXSCRATCH=0 при определении пула хранения таким образом, чтобы чистые тома не использовались.

   - По умолчанию для первичных пулов хранения используется способ совместного размещения по группам. По умолчанию для пулов хранения копий и пулов активных данных совместное размещение отключено. Сервер использует *совместное размещение*, чтобы все файлы, принадлежащие группе клиентских узлов, одному клиентскому узлу, клиентскому файловому пространству или группе клиентских файловых пространств, хранились на минимальном числе томов. При отключенной функции совместного размещения для пула хранения с имеющимися в нем данными клиентов изменение данных в случае разрешения совместного размещения представляет собой непростую задачу.
6. Зарегистрируйте и пометьте тома библиотеки. Следуйте инструкциям в разделах Регистрация томов в автоматизированной библиотеке и Запись меток томов на ленточных томах.

   Убедитесь, что сервер имеет доступ к достаточному количеству томов библиотеки. Поддерживайте запас помеченных томов для предотвращения их дефицита в ходе выполнения какой-либо операции, например резервного копирования клиента. Пометьте дополнительные чистые тома для выполнения в будущем любых возможных операций восстановления.

   Процедуры активации томов и присвоения им меток одинаковы для библиотек, в которых содержатся однотипные или разнотипные накопители. Команду CHECKIN LIBVOLUME можно использовать для регистрации томов, у которых уже есть метки. Или, при желании пометить и зарегистрировать тома за один шаг, введите команду LABEL LIBVOLUME.

   Библиотеки с несколькими типами устройств: Если в вашей библиотеке есть накопители нескольких типов и для сервера IBM Spectrum Protect определено две библиотеки, эти две библиотеки представляют собой одну физическую библиотеку. Для каждой определенной библиотеки активация ленточных томов выполняется отдельно. Убедитесь, что тома включены в правильные библиотеки IBM Spectrum Protect.

Дальнейшие действия

Проверьте определения своих устройств и убедитесь, что все сконфигурировано правильно. Используйте команду QUERY для просмотра информации о каждом объекте хранения.

При проверке результатов выполнения команды QUERY DRIVE убедитесь, что тип устройства для накопителя соответствует ожидаемому. Если путь не задан, тип устройства накопителя будет указан как UNKNOWN, а если используется неправильный путь - будет показан GENERIC_TAPE или другой тип устройства. Этот шаг особенно важен, когда вы используете разные носители.

(Необязательно) Сконфигурируйте совместное использование библиотеки. Следуйте инструкциям в Конфигурирование совместного использования библиотеки.

- Определение ленточных устройств
  Прежде чем вы сможете производить резервное копирование или перенос данных на ленту, вы должны задать ленточное устройство для IBM Spectrum Protect.
- Конфигурирование совместного использования библиотеки
  Несколько серверов IBM Spectrum Protect могут совместно использовать устройства хранения при помощи сети хранения данных. Вы настраиваете один сервер как менеджера библиотеки, а другие серверы - как клиентов библиотеки.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
LABEL LIBVOLUME (запись метки на том библиотеки)
PERFORM LIBACTION (Задать или удалить все накопители и пути для библиотеки)
Информация, связанная с данной:
DEFINE STGPOOL (определение тома в пуле хранения)

Определение ленточных устройств

Прежде чем вы сможете производить резервное копирование или перенос данных на ленту, вы должны задать ленточное устройство для IBM Spectrum Protect.

- Определение библиотек и накопителей
  В ленточной библиотеке может быть один или несколько ленточных накопителей. Узнайте, как задавать библиотеки, накопители и пути к серверу IBM Spectrum Protect.
- Описание классов ленточных устройств
  Класс устройства задает набор характеристик, используемых набором томов, которые можно создать в пуле хранения. Вы должны задать класс устройств для ленточного устройства, чтобы убедиться, что сервер сможет использовать устройство.

Определение библиотек и накопителей

В ленточной библиотеке может быть один или несколько ленточных накопителей. Узнайте, как задавать библиотеки, накопители и пути к серверу IBM Spectrum Protect.

- Определение библиотек
  Перед использованием накопителя следует определить библиотеку, которой он принадлежит.
- Определение носителей
  Чтобы информировать сервер о диске, который может быть использован для доступа к томам хранения, выполните команду DEFINE DRIVE, а затем - команду DEFINE PATH.

Определение библиотек

Перед использованием накопителя следует определить библиотеку, которой он принадлежит.

Процедура

1. Задайте библиотеку, введя команду DEFINE LIBRARY.

   Например, если у вас есть ленточная библиотека IBM TS3500, вы можете задать библиотеку ROBOTMOUNT, используя следующую команду:

   ```
   robotmount robotmount libtype=scsi
   ```

   Если вам требуется совместное использование библиотеки или перемещение данных в режиме без локальной сети, смотрите следующую информацию:
   - Конфигурирование совместного использования библиотеки
   - Конфигурирование перемещения данных в режиме без сети;
2. Задайте путь с сервера к библиотеке, используя команду DEFINE PATH. Задавая параметр DEVICE, укажите имя специального файла устройства. Это имя требуется серверу, чтобы связываться с ленточными накопителями,

устройством со сменой носителей и устройствами со съемными носителями. Дополнительные сведения об именах специальных файлов устройств смотрите в разделе Специальные имена файлов для ленточных устройств.
Операционные системы AIX

```
define path server1 robotmount srctype=server desttype=library
 device=/dev/lb0
```

Операционные системы Linux

```
define path server1 robotmount srctype=server desttype=library
 device=/dev/tsmscsi/lb0
```

Операционные системы Windows

```
define path server1 robotmount srctype=server desttype=library
 device=lb0.0.1.0
```

- Определение библиотек SCSI в сети хранения данных
  Для типа библиотеки SCSI в сети хранения данных сервер может отслеживать серийный номер библиотеки. Используя серийный номер, сервер может идентифицировать устройство при указании пути или использовании устройства.

Информация, связанная с данной:
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (определение пути)

Определение носителей

Чтобы информировать сервер о диске, который может быть использован для доступа к томам хранения, выполните команду DEFINE DRIVE, а затем - команду DEFINE PATH.

Прежде чем начать

Объект накопителя представляет собой механизм в библиотеке, который использует сменный носитель. В случае устройств с несколькими накопителями, включая автоматизированные библиотеки, нужно задать каждый накопитель отдельно и связать его с библиотекой. Определения накопителей могут содержать такие сведения, как адрес элемента для накопителей в библиотеках SCSI, частота очистки ленточных накопителя и состояние подключения накопителя.

IBM Spectrum Protect поддерживает ленточные накопители, которые могут быть автономными или могут быть частью автоматизированной библиотеки. Предпочтительный метод - сконфигурировать ленточное решение с использованием автоматизированных библиотек.

Об этой задаче

При выполнении команды DEFINE DRIVE необходимо указать следующие данные:

Имя библиотеки
: Имя библиотеки, в которой находится накопитель.

Имя носителя
: Имя, назначенное накопителю.

Серийный номер
: Серийный номер накопителя. Параметр серийного номера применяется только для накопителей в SCSI. Используя серийный номер, сервер может подтвердить подлинность устройства при определении пути или использовании устройства сервером.

  При необходимости можно указать серийный номер. По умолчанию сервер получает серийный номер непосредственно с накопителя во время определения пути. Если указан серийный номер, при определении пути к накопителю сервер подтверждает его правильность. Задавая путь, можно задать параметр AUTODETECT=YES, чтобы разрешить серверу корректировать серийный номер, если обнаруженный номер не совпадет с номером, который вы ввели, когда задавали накопитель. Лучше всего задать параметр AUTODETECT=YES, чтобы автоматически обновлять серийный номер для накопителя в базе данных, когда будет создаваться определение пути.

В зависимости от возможностей накопителя, сервер может быть не в состоянии автоматически определить серийный номер. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером. Смотрите раздел Влияние изменений устройств в SAN.

Адрес элемента
: Адрес элемента накопителя. Параметр ELEMENT применяется только для накопителей в библиотеках SCSI. Адрес элемента является числом, указывающим физическое расположение накопителя в автоматизированной библиотеке. Для связывания физического расположения накопителя и SCSI-адреса серверу требуется адрес элемента. Сервер может получить адрес элемента непосредственно с накопителя, когда вы задаете путь, либо номер элемента можно указать, когда вы будете задавать накопитель. Лучше всего задать параметр ELEMENT=AUTODETECT, чтобы сервер автоматически обнаруживал номер элемента, когда вы задаете путь накопителя.

  Возможность автоматического определения сервером адреса элемента зависит от функций библиотеки. В данном случае, если в библиотеке содержится несколько накопителей, при определении накопителя необходимо ввести адрес элемента. Чтобы получить адрес элемента, перейдите в раздел IBM® для IBM Spectrum Protect.

Совет: Драйверы ленточных устройств IBM и драйверы ленточных устройств не IBM генерируют разные файлы и форматы устройств:

- В случае драйверов устройств IBM имена устройств начинаются с rmt, после чего идет целое число, например, /dev/rmt0.
- В случае драйверов ленточных устройств IBM Spectrum Protect имена ленточных устройств начинаются с mt, после чего идет целое число, например, /dev/mt0.

Задавая путь, нужно использовать правильный файл устройства.

Процедура

1. Назначьте накопитель в библиотеку, введя команду DEFINE DRIVE.
2. Чтобы сделать накопитель подходящим для использования сервером, введите команду DEFINE PATH.

   Примеры конфигурирования библиотек, путей и накопителей смотрите в разделах Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей и Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей.

Описание классов ленточных устройств

Класс устройства задает набор характеристик, используемых набором томов, которые можно создать в пуле хранения. Вы должны задать класс устройств для ленточного устройства, чтобы убедиться, что сервер сможет использовать устройство.

Прежде чем начать

Чтобы задать классы устройств, вначале нужно задать для сервера библиотеки и накопители.

Об этой задаче

Список поддерживаемых устройств и допустимых форматов классов устройств смотрите на веб-сайте Поддерживаемые устройства IBM Spectrum Protect для вашей операционной системы:

- Операционные системы AIXОперационные системы WindowsПоддерживаемые устройства для AIX и Windows
- Операционные системы LinuxПоддерживаемые устройства для Linux

Для каждого типа устройств можно задать несколько классов. Например, может понадобиться указать различные атрибуты для разных пулов хранения, в которых используется один и тот же тип накопителя на магнитной ленте. Различия большей частью зависят не от самих устройств, а от того, как их планируется использовать (например, от задержек демонтирования или лимитов монтирования).

Рекомендации:

- Один класс устройств может быть связан с несколькими пулами хранения, в то время как каждый пул хранения может быть связан только с одним классом устройства.
- В SCSI-библиотеки могут входить ленточные накопители нескольких типов. При описании класса устройств в этой среде необходимо объявить значение параметра FORMAT.

  Дополнительную информацию смотрите в разделе Смешанные типы устройств в библиотеке.

Процедура

Чтобы задать класс устройств, введите команду DEFINE DEVCLASS с параметром DEVTYPE; эта команда назначает классу устройства тип устройства.

Результаты

Если опция DEVCONFIG содержится в файле dsmserv.opt, указанные с этой опцией файлы будут автоматически изменяться по результатам команд DEFINE DEVCLASS, UPDATE DEVCLASS и DELETE DEVCLASS.

- Как задать классы устройств LTO
  Чтобы предотвратить проблемы при одновременном использовании разных поколений накопителей LTO и носителей в одной библиотеке, смотрите ограничения. Также ознакомьтесь с ограничениями для шифрования накопителей LTO.
- Как задать классы устройств 3592
  Определения класса устройств для 3592, TS1130, TS1140, TS1150 и более поздних устройств включают параметры для ускоренного доступа к томам и шифрованием на носителях. Чтобы избежать проблем при комбинировании разных поколений накопителей 3592 и TS1130 и новее, ознакомьтесь с рекомендациями.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
Команда QUERY DEVCLASS (отображение информации об одном или нескольких классах устройств)
UPDATE DEVCLASS (изменение класса устройства)

Как задать классы устройств LTO

Чтобы предотвратить проблемы при одновременном использовании разных поколений накопителей LTO и носителей в одной библиотеке, смотрите ограничения. Также ознакомьтесь с ограничениями для шифрования накопителей LTO.

- Использование разных поколений накопителей и устройств LTO в библиотеке
  При одновременном использовании разных поколений накопителей и носителей LTO надо учитывать возможности каждого поколения с точки зрения чтения и записи. Предпочтительнее сконфигурировать разные классы устройств для каждого поколения носителей.
- Предельное число точек монтирования в средах со смешанными типами носителей LTO
  В библиотеке со смешанными типами носителей, в которой несколько классов устройств указывают на одну библиотеку, совместимые накопители совместно используются пулами хранения. Убедитесь, что для параметра MOUNTLIMIT в каждом из классов устройств задано подходящее значение.
- Как включить и выключить шифрование накопителей для ленточных накопителей LTO поколения 4 или новее
  IBM Spectrum Protect поддерживает три типа шифрования накопителей, которые доступны для накопителей LTO поколения 4 или новее: шифрование на уровне приложений, системы и библиотеки (Приложение, Система и Библиотека). Эти методы конфигурируются на аппаратном уровне.

Использование разных поколений накопителей и устройств LTO в библиотеке

При одновременном использовании разных поколений накопителей и носителей LTO надо учитывать возможности каждого поколения с точки зрения чтения и записи. Предпочтительнее сконфигурировать разные классы устройств для каждого поколения носителей.

Об этой задаче

Если предполагается совместная работа различных поколений накопителей и носителей LTO, обратите внимание на следующие ограничения:

Табл. 1. Функции чтения-записи для накопителей LTO различных поколений

Накопители	Носитель 1-го поколения	Носитель 2-го поколения	Носитель 3-го поколения	Носитель 4-го поколения	Носители поколения 5	Носители поколения 6	Носители поколения 7	Носители поколения M8	Носители поколения 8
Поколение 1	Доступ чтение/запись	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 2	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 3	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 4	неприменимо	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 5	неприменимо	неприменимо	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 6	неприменимо	неприменимо	неприменимо	Доступ только для чтения	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо	неприменимо
Поколение 7	неприменимо	неприменимо	неприменимо	неприменимо	Права чтения	Доступ чтение/запись	Доступ чтение/запись	неприменимо	неприменимо
Поколение 8	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	неприменимо	Доступ чтение/запись	Доступ чтение/запись	Доступ чтение/запись

Пример

При совместном использовании накопителей и носителей различных типов сконфигурируйте разные классы устройств - по одному на каждый тип носителя. Чтобы задать тип носителя, используйте параметр FORMAT в каждом из определений классов устройств. Не указывайте FORMAT=DRIVE. Например, если используются накопители Ultrium поколения 5 и Ultrium поколения 6, задайте FORMAT=ULTRIUM5C (или ULTRIUM5) для класса устройств Ultrium поколения 5 и FORMAT=ULTRIUM6C (или ULTRIUM6) для класса устройств Ultrium поколения 6.

В этом примере оба класса устройств могут указать на одну и ту же библиотеку с накопителями Ultrium поколения 5 и Ultrium поколения 6. Накопители совместно используются между двумя пулами хранения. В одном пуле хранения используется первый класс устройства и исключительно носители Ultrium поколения 5. В другом пуле хранения используется второй класс устройства и только носители Ultrium поколения 6. Поскольку два пула хранения совместно используют одну библиотеку, носители Ultrium поколения 5 могут монтироваться в накопители Ultrium поколения 6, если они станут доступны во время обработки точки монтирования.

Если библиотека содержит и более старые поколения носителей 'только для чтения', и более новые носители 'чтение/запись', то нужно пометить носители 'только для чтения' как 'только для чтения' и зарезервировать все чистые носители 'только для чтения'. Например, если в одной библиотеке одновременно используются накопители и носители Ultrium поколений 4 и 6, то необходимо пометить носитель поколения 4 как доступный только для чтения. Кроме того, надо зарезервировать все чистые тома поколения 4.

Предельное число точек монтирования в средах со смешанными типами носителей LTO

В библиотеке со смешанными типами носителей, в которой несколько классов устройств указывают на одну библиотеку, совместимые накопители совместно используются пулами хранения. Убедитесь, что для параметра MOUNTLIMIT в каждом из классов устройств задано подходящее значение.

Например, в смешанной библиотеке носителей, которая содержит накопители и носители Ultrium поколений 1 и 2, носитель Ultrium поколения 1 можно смонтировать на накопителях Ultrium поколения 2.

Рассмотрим пример смешанной библиотеки, которая включает в себя следующие накопители и носители:

- Четыре накопителя LTO Ultrium поколения 1 и носители LTO Ultrium поколения 1
- Четыре накопителя LTO Ultrium поколения 2 и носители LTO Ultrium поколения 2

ВЫ создали следующие классы устройств:

- Класс устройств LTO Ultrium поколения 1 с именем LTO1CLASS, для которого задан параметр FORMAT=ULTRIUM1C
- Класс устройств LTO Ultrium поколения 2 с именем LTO2CLASS, для которого задан параметр FORMAT=ULTRIUM2C

Вы также создали следующие пулы хранения:

- Пул хранения LTO Ultrium поколения 1 — LTO1POOL на основе класса устройства LTO1CLASS
- Пул хранения LTO Ultrium поколения 2 — LTO2POOL на основе класса устройства LTO2CLASS

Количество точек монтирования, доступных для использования в каждом пуле хранения, указывается в классе устройства при помощи параметра MOUNTLIMIT. Для параметра MOUNTLIMIT в классе устройства LTO2CLASS должно быть установлено значение 4, соответствующее количеству доступных накопителей, в которые могут быть смонтированы только носители LTO7. Для параметра MOUNTLIMIT в классе устройства LTO1CLASS должно быть задано значение, превышающее число доступных накопителей (5 или, возможно, 6), чтобы скорректировать тот факт, что носители Ultrium поколения 1 могут монтироваться в накопители Ultrium поколения 7. Оптимальное значение MOUNTLIMIT зависит от рабочей нагрузки и шаблонов доступа к пулу хранения.

Следите за значением параметра MOUNTLIMIT и регулируйте его в соответствии с изменениями рабочей нагрузки. Если для параметра MOUNTLIMIT пула LTO1POOL установлено высокое значение, то запросы на монтирование от пула LTO2POOL могут откладываться или завершаться неудачно, поскольку накопители Ultrium поколения 2 используются для выполнения запросов на монтирование носителей Ultrium поколения 1. В наихудшем случае большое количество конфликтов накопителей Ultrium поколения 2 может вызвать ошибки монтирования носителей поколения 2, сопровождающиеся сообщением:

```
ANR8447E В библиотеке нет доступных накопителей.
```

Если для параметра MOUNTLIMIT пула LTO1POOL задано слишком малое значение, требования монтирования, которые могли бы быть выполнены накопителями LTO Ultrium поколения 2, будут задержаны.
Ограничение: При совместном использовании накопителей Ultrium поколения 1 и поколения 2 или 3 применяются ограничения из-за выделения точек монтирования. Например, процессы, для которых требуется несколько точек монтирования томов Ultrium поколений 1 и 2, могут пытаться зарезервировать накопители Ultrium поколения 2, даже если монтирование может быть выполнено доступным накопителем Ultrium поколения 6. Процессы, которые выполняются таким образом, включают команды MOVE DATA и BACKUP STGPOOL. Эти процессы будут ожидать, пока нужное число точек монтирования не будет получено на накопителях Ultrium поколения 2.
Ссылки, связанные с данной:
BACKUP STGPOOL (резервное копирование данных основного пула хранения в пул хранения копий)
DEFINE DEVCLASS (Задать класс устройств)
MOVE DATA (Переместить файлы в том пула хранения)

Как включить и выключить шифрование накопителей для ленточных накопителей LTO поколения 4 или новее

IBM Spectrum Protect поддерживает три типа шифрования накопителей, которые доступны для накопителей LTO поколения 4 или новее: шифрование на уровне приложений, системы и библиотеки (Приложение, Система и Библиотека). Эти методы конфигурируются на аппаратном уровне.

Об этой задаче

Параметр DRIVEENCRYPTION в команде DEFINE DEVCLASS указывает, разрешено ли шифрование накопителей для форматов IBM и HP LTO поколения 4 или новее, Ultrium 4 и Ultrium 4C. Этот параметр обеспечивает совместимость IBM

Spectrum Protect с настройками аппаратного шифрования пустых томов. Использовать этот параметр для заполненных или заполняющихся томов пула хранения нельзя.

IBM Spectrum Protect поддерживает метод шифрования на уровне приложений для накопителей IBM и HP LTO-4 или новее. Методы шифрования на уровне системы и библиотеки поддерживаются только накопителями IBM LTO-4 или новее. Метод шифрования на уровне библиотеки поддерживается, только если его поддерживает оборудование вашей системы (например IBM TS3500).

Ограничение: Использовать шифрование накопителей при работе с носителями с одноразовой записью и многократным чтением (Write-Once, Read-Many - WORM) нельзя.

Метод шифрования на уровне приложения задается на аппаратном уровне. Чтобы воспользоваться методом шифрования на уровне программы, при котором IBM Spectrum Protect создает ключи шифрования и управляет ими, задайте для параметра DRIVEENCRYPTION значение ON. При этом включается шифрование данных для пустых томов. Если для этого параметра задано значение ON, а в оборудовании используется другой метод шифрования, операции резервного копирования будут завершаться с ошибкой.

Процедура

Следующий упрощенный пример показывает, какие шаги нужно выполнить, чтобы включить и выключить шифрование данных на пустых томах в пуле хранения:

1. Задайте библиотеку, введя команду DEFINE LIBRARY:

   ```
   define library 3584 libtype=SCSI
   ```

2. Задайте класс устройств LTO_ENCRYPT, введя команду DEFINE DEVCLASS и указав IBM Spectrum Protect в качестве менеджера ключей:

   ```
   define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
   ```

3. Задайте пул хранения, введя команду DEFINE STGPOOL:

   ```
   define stgpool lto_encrypt_pool lto_encrypt
   ```

4. Чтобы отключить шифрование новых томов, установите для параметра DRIVEENCRYPTION значение OFF. Значение по умолчанию - ALLOW. Шифрование пустых томов на уровне накопителя доступно, если включен другой метод шифрования.

Понятия, связанные с данным:
Методы шифрования лент

Как задать классы устройств 3592

Определения класса устройств для 3592, TS1130, TS1140, TS1150 и более поздних устройств включают параметры для ускоренного доступа к томам и шифрованием на носителях. Чтобы избежать проблем при комбинировании разных поколений накопителей 3592 и TS1130 и новее, ознакомьтесь с рекомендациями.

- Использование носителей 3592 разных поколений в одной библиотеке
  Для достижения оптимальной производительности не используйте носители 3592 разных поколений в одной библиотеке. При использовании разных поколений накопителей могут возникнуть ошибки носителей. Например, IBM Spectrum Protect может не прочитать метку тома.
- Управление скоростью доступа к данным для томов в классе устройств 3592
  При создании томов можно оптимизировать емкость хранения и повысить скорость доступа к данным. Разбивая данные на пулы хранения, в которых есть тома, вы можете задать процент масштабируемой емкости, чтобы обеспечить максимальную емкость хранения или быстрый доступ к тому.
- Как включить и выключить шифрование накопителей 3592 поколения 2 и новее
  При работе с IBM Spectrum Protect можно использовать следующие типы шифрования накопителей для накопителей 3592 второго и последующих поколений: шифрование на уровне программ, системы и библиотеки. Эти методы конфигурируются на аппаратном уровне.

Использование носителей 3592 разных поколений в одной библиотеке

Для достижения оптимальной производительности не используйте носители 3592 разных поколений в одной библиотеке. При использовании разных поколений накопителей могут возникнуть ошибки носителей. Например, IBM Spectrum Protect может не прочитать метку тома.

Об этой задаче

В следующей таблице показана функциональная совместимость поколений накопителей в отношении чтения и записи.

Накопители	Формат первого поколения	Формат второго поколения	Формат третьего поколения	Формат четвертого поколения	Носители поколения 5
Поколение 1	Доступ чтение/ запись	неприменимо	неприменимо	неприменимо	неприменимо
Поколение 2	Доступ чтение/ запись	Доступ чтение/ запись	неприменимо	неприменимо	неприменимо
Поколение 3	Доступ только для чтения	Доступ чтение/ запись	Доступ чтение/ запись	неприменимо	неприменимо
Поколение 4	неприменимо	Только для чтения	Доступ чтение/ запись	Доступ чтение/ запись	неприменимо
Поколение 5	неприменимо	неприменимо	Права чтения	Доступ чтение/ запись	Доступ чтение/ запись

Если вам нужно смешивать поколения накопителей в библиотеке, рассмотрите пример и ограничения, чтобы это помогло вам предотвратить проблемы.

Табл. 1. Использование накопителей разных поколений

Тип библиотеки	Пример и ограничения

Тип библиотеки	Пример и ограничения
SCSI	Задайте новый пул хранения и класс устройств для последнего поколения носителей. Например, пусть у вас есть пул хранения и класс устройств для 3592-2. Пул хранения содержит все носители, записанные в формате поколения 2. Предположим, что в определении класса устройств для параметра FORMAT задано значение 3952-2 (не FORMAT). Вы добавляете в библиотеку накопители поколения 3. Сделайте следующее: 1. В новом определении класса устройств для накопителей поколения 3 задайте для параметра FORMAT значение 3592-3 или 3592-3C. Не задавайте значение DRIVE. 2. В определении пула хранения, связанного с накопителями поколения 2, обновите параметр MAXSCRATCH до 0, например: `update stgpool genpool2 maxscratch=0` При таком методе оба поколения смогут использовать оптимальный для себя формат, и можно будет свести к минимуму потенциальные ошибки носителей, связанные с использованием разных поколений. Однако он не разрешает всех проблем с носителями. Например, возможны конфликты точек монтирования и ошибки монтирования. (Чтобы подробнее узнать о конкуренции точек монтирования в контексте накопителей 3592 и носителей, смотрите раздел Как задать классы устройств 3592.) Ограничение: Ниже описаны ограничения, действующие в отношении носителей: • CHECKIN LIBVOL: При использовании опции CHECKLABEL=YES существует неразрешенная проблема. Если метка записывается в формате поколения 3 или новее и вы зададите опцию CHECKLABEL=YES, накопители предыдущих поколений не будут работать при использовании этой команды. Во избежание проблем задайте CHECKLABEL=BARCODE. • LABEL LIBVOL: Когда сервер пытается использовать накопители предыдущего поколения для чтения метки, записаннов в формате поколения 3 или новее, команда LABEL LIBVOL завершится неудачно, если не задан параметр OVERWRITE=YES. Убедитесь, что на носителе, для которого указано OVERWRITE=YES, нет никаких активных данных. • CHECKOUT LIBVOL: Когда IBM Spectrum Protect проверяет метку (CHECKLABEL=YES) как формат поколения 3 или новее и читает некопители предыдущих поколений, команда завершается неудачно. Во избежание этой проблемы задайте CHECKLABEL=NO.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
CHECKOUT LIBVOLUME (исключение тома хранения из библиотеки)
LABEL LIBVOLUME (запись метки на том библиотеки)
UPDATE STGPOOL (обновить пул хранения)

Управление скоростью доступа к данным для томов в классе устройств 3592

При создании томов можно оптимизировать емкость хранения и повысить скорость доступа к данным. Разбивая данные на пулы хранения, в которых есть тома, вы можете задать процент масштабируемой емкости, чтобы обеспечить максимальную емкость хранения или быстрый доступ к тому.

Об этой задаче

Чтобы уменьшить емкость носителей, задайте параметр SCALECAPACITY, когда будете задавать класс устройств с использованием команды DEFINE DEVCLASS или когда будете обновлять класс устройств с использованием команды UPDATE DEVCLASS.

Задайте значение в процентах, равное 20, 90 или 100. Значение, равное 20 процентам, обеспечит самый быстрый доступ к данным, а 100 процентам - самую большую емкость для хранения данных. Например, если вы укажете масштабирование емкости, составляющее 20%, для класса устройств 3592 (без сжатия), емкость тома формата 3592 в устройстве этого класса будет составлять 20% от полной емкости, равное 300 ГБ (около 60 ГБ).

Масштабирование емкости действует только при первой записи данных на том. Никакие изменения класса устройств с целью масштабирования емкости не повлияют на тома, если на них уже записаны данные, пока том не будет переведен в чистое состояние.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Как включить и выключить шифрование накопителей 3592 поколения 2 и новее

При работе с IBM Spectrum Protect можно использовать следующие типы шифрования накопителей для накопителей 3592 второго и последующих поколений: шифрование на уровне программ, системы и библиотеки. Эти методы конфигурируются на аппаратном уровне.

Об этой задаче

Параметр DRIVEENCRYPTION в команде DEFINE DEVCLASS указывает, разрешено ли шифрование накопителей для накопителей 3592 поколения 2 и новее. Используйте этот параметр для обеспечения совместимости IBM Spectrum Protect с настройками аппаратного шифрования пустых томов. Использовать этот параметр для заполненных или заполняющихся томов пула хранения нельзя.

- Чтобы воспользоваться методом шифрования на уровне программы, при котором IBM Spectrum Protect создает ключи шифрования и управляет ими, задайте для параметра DRIVEENCRYPTION значение ON. Это позволяет шифровать данные на пустых томах. Если для параметра задано значение ON, а устройство сконфигурировано для использования другого метода шифрования, операции резервного копирования будут завершаться неудачно.
- Чтобы использовать методы шифрования на уровне библиотеки или системы, установите для параметра значение ALLOW. Таким образом, IBM Spectrum Protect не будет управлять шифрованием накопителей, но даст возможность оборудованию шифровать данные на томе одним из других методов. Указание этого параметра не означает автоматического шифрования дисков. Данные могут шифроваться только путем указания параметра ALLOW и конфигурирования оборудования на один из этих методов.

Параметр DRIVEENCRYPTION является необязательным. Значение по умолчанию позволяет использовать методы шифрования на уровне библиотеки или системы.

Процедура

В приведенном ниже упрощенном примере показано, как, используя IBM Spectrum Protect в качестве менеджера ключей, зашифровать данные на пустых томах в пуле хранения:

1. Задайте библиотеку, введя команду DEFINE LIBRARY. Например, введите следующую команду:

   ```
   define library 3584 libtype=SCSI
   ```

2. Задайте класс устройств, 3592_ENCRYPT, введя команду DEFINE DEVCLASS и задав значение ON для параметра DRIVEENCRYPTION. Например, введите следующую команду:

   ```
   define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
   ```

3. Задайте пул хранения. Например, введите следующую команду:

   ```
   define stgpool 3592_encrypt_pool 3592_encrypt
   ```

Дальнейшие действия

Чтобы отключить все методы шифрования новых томов, установите для параметра DRIVEENCRYPTION значение OFF. Если оборудование сконфигурировано на шифрование данных на уровне библиотеки или системы, а для параметра DRIVEENCRYPTION установлено значение OFF, операции резервного копирования данных будут завершаться с ошибкой.

Конфигурирование совместного использования библиотеки

Несколько серверов IBM Spectrum Protect могут совместно использовать устройства хранения при помощи сети хранения данных. Вы настраиваете один сервер как менеджера библиотеки, а другие серверы - как клиентов библиотеки.

Прежде чем начать

Убедитесь, что ваши системы соответствуют требованиям лицензирования для совместного использования библиотек. Для каждого сервера IBM Spectrum Protect, сконфигурированного в качестве клиента библиотеки или менеджера библиотеки в среде SAN, требуется предоставленное право на IBM Spectrum Protect for SAN.

Об этой задаче

При перемещении данных в режиме без локальной сети клиентские системы IBM Spectrum Protect могут непосредственно обратиться к устройствам хранения, определенным для сервера IBM Spectrum Protect. Для выполнения перемещения данных агенты хранения устанавливаются и конфигурируются в клиентских системах.

Чтобы сконфигурировать совместное использование библиотеки, необходимо определить один сервер IBM Spectrum Protect как менеджер библиотеки для вашей конфигурации библиотеки совместного использования. Затем вы задаете другие серверы IBM Spectrum Protect как клиенты библиотеки, связывающиеся с менеджером библиотеки и запрашивающие у него ресурсы хранения. Сервер менеджера библиотеки должен быть той же версии или новее, чем сервер или серверы, определенные как клиенты библиотеки.

Процедура

Чтобы обеспечить совместное использование ресурсов библиотеки в SAN на серверах IBM Spectrum Protect, выполните следующие шаги:

1. Установить связь между серверами.

   Чтобы совместно использовать устройство хранения в сети хранения данных (SAN), определите серверы друг для друга при помощи функции перекрестного определения. У каждого сервера должно быть уникальное имя.

2. Задайте библиотеку совместного использования и сконфигурируйте ленточные устройства в системах серверов.

   Используйте процедуру, описанную в разделе Конфигурирование библиотек для использования сервером, чтобы определить библиотеку для среды совместного использования. Измените процедуру для определения библиотеки как совместно используемой, задав параметр SHARED=YES для команды DEFINE LIBRARY.

3. Определите сервер менеджера библиотеки.
4. Задайте совместно используемую библиотеку на сервере, который является клиентом библиотеки.
5. На сервере менеджера библиотеки определите пути от клиента библиотеки к каждому носителю, доступному для клиента библиотеки. Имя устройства должно отражать способ, по которому система клиента библиотеки распознает это ленточное устройство. Пути от менеджера библиотеки к каждому ленточному накопителю должны определяться в том порядке, в каком клиент библиотеки будет использовать эти накопители.

   Чтобы избежать проблем убедитесь, что все пути накопителей, заданные для менеджера библиотеки, также заданы для каждого клиента библиотеки.

   Например, если в менеджере библиотеки заданы три ленточных накопителя, на клиенте библиотеки также должны быть заданы три ленточных накопителя. Чтобы ограничить число накопителей, которые клиент библиотеки может использовать одновременно, используйте параметр MOUNTLIMIT для класса устройств на клиенте библиотеки.
6. Определите классы устройств для совместно используемой библиотеки.

   Рекомендуется задавать одинаковые имена классов устройств на обоих серверах, чтобы исключить путаницу при определении нескольких классов устройств одного типа с одинаковыми параметрами библиотеки. Некоторые операции, такие как резервное копирование базы данных, используют имя класса устройства для идентификации данных для резервного копирования.

   Параметры класса устройств, заданные в менеджере библиотеки, переопределяют параметры, заданные для клиента библиотеки. Если имена классов устройств различаются, менеджер библиотеки использует параметры, указанные в классе устройства, который соответствует типу устройства, указанному для клиента библиотеки.

7. Определите пул хранения для совместно используемой библиотеки.
8. Повторите эти шаги, чтобы сконфигурировать другой сервер в качестве клиента библиотеки.

- Операционные системы AIXОперационные системы LinuxПример: Совместное использование библиотек для серверов AIX и Linux
  Чтобы узнать, как настроить среду совместного использования библиотек SCSI для серверов, работающих в системах AIX или Linux, смотрите пример процедуры.
- Пример: Совместное использование библиотек для серверов Windows
  Чтобы узнать, как настроить среду совместного использования библиотек для серверов, работающих в системах Windows, ознакомьтесь с примером процедуры.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
DEFINE LIBRARY (Задать библиотеку)
DEFINE STGPOOL (определение тома в пуле хранения)
Операционные системы AIXОперационные системы Linux

Пример: Совместное использование библиотек для серверов AIX и Linux

Чтобы узнать, как настроить среду совместного использования библиотек SCSI для серверов, работающих в системах AIX или Linux, смотрите пример процедуры.

Об этой задаче

В этом примере конфигурируется сервер менеджера библиотеки с именем ASTRO и клиент библиотеки с именем JUDY. Для подсказки, где какой шаг используется, командам предшествует имя сервера, на котором их нужно вводить. Большинство команд вводится в клиенте библиотеки.

Для библиотек SCSI задайте библиотеку, указав параметр libtype=scsi.

Процедура

1. Чтобы сконфигурировать ASTRO как сервер менеджера библиотеки, определите библиотеку совместного использования SCSI с именем SANGROUP. Например:

   ```
   astro> define library sangroup libtype=scsi shared=yes
   ```

   Затем выполните остальные шаги, как описано в разделе Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей, чтобы сконфигурировать библиотеку.
   Совет: Команду PERFORM LIBACTION можно использовать для определения накопителей и нутей для библиотеки в один шаг.
2. Определите ASTRO как сервер менеджера библиотеки, введя команду DEFINE SERVER.

   ```
   judy> define server astro serverpassword=secret hladdress=192.0.2.24
    lladdress=1777 crossdefine=yes
   ```

3. Определите библиотеку совместного использования SANGROUP, введя команду DEFINE LIBRARY. Необходимо использовать имя сервера менеджера библиотеки в параметре PRIMARYLIBMANAGER и равенство `LIBTYPE=SHARED`.

   ```
   judy> define library sangroup libtype=shared primarylibmanager=astro
   ```

   Убедитесь, что имя библиотеки совпадает с именем библиотеки, указанным в менеджере библиотеки.
4. Определите пути от менеджера библиотеки ASTRO к двум накопителям в библиотеке совместного использования, введя команду DEFINE PATH.
   Операционные системы AIX

   ```
   astro> define path judy drivea srctype=server desttype=drive
    library=sangroup device=/dev/rmt6
   astro> define path judy driveb srctype=server desttype=drive
    library=sangroup device=/dev/rmt7
   ```

   Операционные системы Linux

```
astro> define path judy drivea srctype=server desttype=drive
 library=sangroup device=/dev/IBMtape6
astro> define path judy driveb srctype=server desttype=drive
 library=sangroup device=/dev/IBMtape7
```

5. Определите все классы устройств, связанные с данной совместно используемой библиотекой.
   Операционные системы AIX

   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Операционные системы Linux

   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Следующие параметры определения класса устройств должны быть одинаковы для клиента библиотеки и для менеджера библиотеки:
   - LIBRARY
   - DRIVEENCRYPTION
   - WORM
   - FORMAT
6. Определите пул хранения с именем BACKTAPE для библиотеки совместного использования, которая будет использоваться. Введите команду DEFINE STGPOOL.

   ```
   judy> define stgpool backtape tape maxscratch=50
   ```

Дальнейшие действия

Повторите эту процедуру для определения других клиентов библиотеки для вашего менеджера библиотеки.
Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
DEFINE DRIVE (Задать накопитель для библиотеки)
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (определение пути)
DEFINE STGPOOL (определение тома в пуле хранения)
Операционные системы Windows

Пример: Совместное использование библиотек для серверов Windows

Чтобы узнать, как настроить среду совместного использования библиотек для серверов, работающих в системах Windows, ознакомьтесь с примером процедуры.

Об этой задаче

В этом примере конфигурируется сервер менеджера библиотеки с именем ASTRO и клиент библиотеки с именем JUDY.

Для библиотек SCSI задайте библиотеку, указав параметр libtype=scsi.

- Операционные системы WindowsНастройка сервера менеджера библиотеки
  Вы должны настроить сервер менеджера библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.
- Операционные системы WindowsУстановка серверов клиентов библиотеки
  Нужно настроить один или нескольк серверовклиента библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.

Операционные системы Windows

Настройка сервера менеджера библиотеки

Вы должны настроить сервер менеджера библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.

Процедура

Следующая процедура - это пример того, как задать сервер IBM Spectrum Protect с именем ASTRO в качестве менеджера библиотек:

1. Убедитесь, что сервер менеджера библиотек работает:
   a. Запустите консоль управления службами Windows (services.msc).
   b. Выберите службу. Например, `TSM Server1`.
   c. Если служба не работает, то щелкните правой кнопкой мыши по имени службы и щелкните по Пуск.
2. Получите информацию о библиотеке и драйвере для устройства совместно используемой библиотеки:
   a. Запустите файл `tsmdlst.exe`. Эта утилита находится в каталоге \Program Files\Tivoli\TSM\server.
3. Задайте тип библиотеки SCSI. Например:

   ```
   define library sangroup libtype=scsi shared=yes
   ```

   В данном примере используется стандартный серийный номер библиотеки, то есть сервер получает номер из самой библиотеки при определения пути. Возможность автоматического определения сервером серийного номера зависит от функций библиотеки. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером.

4. Задайте для сервера путь к библиотеке:

   ```
   define path astro sangroup srctype=server desttype=library
    device=lb0.0.0.2
   ```

   Если при определении библиотеки не указан серийный номер, сервер отправит запрос библиотеке, чтобы получить эти данные. Если при определении библиотеки был указан серийный номер, сервер проверит указанную информацию и в случае несовпадения выведет соответствующее сообщение.

5. Определите накопители в библиотеке.

   ```
   define drive sangroup drivea
   define drive sangroup driveb
   ```

   В данном примере используется стандартная процедура получения серийного номера накопителя, то есть сервер получает серийный номер из самой библиотеки во время определения пути. В зависимости от возможностей накопителя, сервер может быть не в состоянии автоматически определить серийный номер. В этом случае сервер не запишет серийный номер устройства и не сможет подтвердить идентичность устройства при определении пути или использовании носителя сервером.

   В данном примере также используется стандартный адрес элемента накопителя, который сервер получает непосредственно с диска во время определения пути.

   Адрес элемента является числом, указывающим физическое расположение накопителя в автоматизированной библиотеке. Для связывания физического расположения накопителя и SCSI-адреса серверу требуется адрес элемента. Сервер может получить номер элемента непосредственно с носителя во время определения пути, или его можно указать при определении носителя.

   Возможность автоматического определения сервером адреса элемента зависит от функций библиотеки. В этом случае при определении носителя нужно ввести адрес элемента. Номера элементов для многих библиотек можно найти на сайте IBM® для IBM Spectrum Protect.

6. Задайте путь от сервера к каждому диску.

   ```
   define path astro drivea srctype=server desttype=drive library=sangroup
    device=mt0.1.0.2
   define path astro driveb srctype=server desttype=drive library=sangroup
    device=mt0.2.0.2
   ```

   Если при определении накопителя не был указан серийный номер или адрес элемента, сервер направит запрос библиотеке, чтобы получить эти данные.

7. Задайте хотя бы один класс устройств.

   ```
   define devclass tape devtype=dlt library=sangroup
   ```

8. Добавить в перечень библиотеки. В следующем примере выполняется регистрация всех томов в перечне библиотеки в качестве чистых томов. Сервер использует имя на метке штрих-кода в качестве имени тома.

```
checkin libvolume sangroup search=yes status=scratch
 checklabel=barcode
```

9. Настройте пул хранения для совместно используемой библиотеки, содержащей не более 50 чистых томов.

```
define stgpool backtape tape
 description='storage pool for shared sangroup' maxscratch=50
```

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
DEFINE DRIVE (Задать накопитель для библиотеки)
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (определение пути)
DEFINE STGPOOL (определение тома в пуле хранения)
Операционные системы Windows

Установка серверов клиентов библиотеки

Нужно настроить один или нескольк серверовклиента библиотеки, чтобы сконфигурировать серверы IBM Spectrum Protect для совместного использования устройств, подключенных к SAN.

Прежде чем начать

Убедитесь, что сервер менеджера библиотек задан.

Об этой задаче

Нужно задать сервер менеджера библиотеки. Ниже приведен пример процедуры настройки сервера IBM Spectrum Protect с именем JUDY в качестве клиента библиотеки.

Процедура

1. Убедитесь, что сервер менеджера библиотек работает:
   a. Запустите консоль управления службами Windows (services.msc).
   b. Выберите службу. Например, `TSM Server1`.
   c. Если служба не работает, то щелкните правой кнопкой мыши по имени службы и выберите Пуск.
2. Получите информацию о библиотеке и драйвере для устройства совместно используемой библиотеки:
   a. Запустите файл `tsmdlst.exe`. Эта утилита находится в каталоге \Program Files\Tivoli\TSM\server.
3. Задайте совместно используемую библиотеку, SANGROUP, и укажите менеджер библиотеки. Убедитесь, что имя библиотеки совпадает с именем библиотеки, указанным в менеджере библиотеки.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Задайте пути от сервера клиента библиотеки до каждого из накопителей, введя команды на административном клиенте:

```
define path judy drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.3
 define path judy driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.3
```

5. Задайте хотя бы один класс устройств, введя команды с клиента библиотеки:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10
library=sangroup
```

Параметры класса устройства для клиента библиотеки задайте равными параметрам, установленным для менеджера библиотеки. Задание одинаковых имен классов устройств на обоих серверах рекомендуется, но не является обязательным.

Параметры класса устройств, заданные на сервере менеджера библиотек переопределяют параметры, заданные для клиента библиотеки. Это правило действует независимо от того, имеют ли классы устройств одинаковые имена

на обоих серверах. Если имена классов устройств различаются, менеджер библиотеки использует параметры, указанные в классе устройства, совпадающем с типом устройства, заданным для клиента библиотеки.

Если необходимо, чтобы какой-либо параметр клиента библиотеки имел значение, отличающееся от значения параметра класса устройства менеджера библиотеки (например, лимит монтирования), то сделайте следующее:

a. Создайте дополнительный класс устройства на сервере менеджера библиотеки. Укажите нужные значения параметров для клиента библиотеки.
b. Создайте класс устройства на клиенте библиотеки с таким же именем и типом устройства, как у нового класса устройства, созданного на сервере библиотеки.

6. Задайте пул хранения (BACKTAPE) для совместно используемой библиотеки:

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

7. Повторите эту операцию, чтобы задать дополнительные сервера как клиенты библиотеки.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (определение пути)
DEFINE STGPOOL (определение тома в пуле хранения)

Настройка иерархии пулов хранения

В ходе процесса реализации вы должны настроить иерархию пулов хранения. Настройте хотя бы один первичный пул хранения на диске и один первичный пул хранения на ленте. Убедитесь, что ежедневно осуществляется перенос данных с диска на ленту.

Прежде чем начать

1. Убедитесь, что вы ознакомились с информацией в Планирование иерархии пулов хранения.
2. Убедитесь, что для резервного копирования данных клиента заданы соответствующие правила, которые также называются *политикой*. Следуйте инструкциям в Как задать роли для резервного копирования и архивирования данных клиента.
3. Убедитесь, что политика назначена для каждого узла. Инструкций по назначению политики при регистрации узла смотрите в разделе Регистрация клиентов.

Процедура

Чтобы настроить иерархию пулов хранения, выполните следующие шаги:

1. Задайте первичный пул хранения для ленточного устройства, введя команду DEFINE STGPOOL.

   Например, задайте первичный пул хранения TAPE1 с классом устройств LTO и включите совместное размещение группы. Задайте максимальное число чистых томов, которые сервер может потребовать для данного пула хранения, равное 999. Введите следующую команду:

```
define stgpool tape1 lto pooltype=primary collocate=group
maxscratch=999
```

2. Задайте накопители, пути и библиотеки для первичного пула хранения на ленте. Следуйте инструкциям в Определение ленточных устройств.
3. Задайте первичный пул хранения для дискового устройства, введя команду DEFINE STGPOOL.

   Например, задайте пул хранения DISK1 с классом устройств FILE. Убедитесь, что данные можно переносить в ленточный пул хранения, TAPE1, но запретите автоматический перенос, задав значение 100 для параметра HIGHMIG и значение 0 для параметра LOWMIG. Запретите высвобождение пространства, задав значение 100 для параметра RECLAIM. Включите совместное размещение для узлов. Задайте максимальное число чистых томов, которые сервер может потребовать для данного пула хранения, равное 9999. Используйте параметр MIGPROCESS, чтобы задать число процессов переноса. Значение параметра MIGPROCESS должно равняться числу накопителей в библиотеке минус число накопителей, зарезервированных для операций восстановления. Введите следующую команду:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Дополнительную информацию о том, как настроить перенос с диска на ленту, смотрите в разделе Перенос дисковых пулов хранения.

Дальнейшие действия

Иерархия пула хранения содержит только первичные пулы хранения. После настройки иерархии пулов хранения выполните следующие шаги:

1. Создайте пул хранения копий на ленточном устройстве. Инструкции смотрите в разделе DEFINE STGPOOL (определение пула хранения копий, которому назначены устройства с последовательным доступом).
2. Создайте резервную копию первичного пула хранения на основе лент в пуле хранения копий, используя команду BACKUP STGPOOL. Инструкции смотрите в разделе BACKUP STGPOOL (резервное копирование данных основного пула хранения в пул хранения копий).
3. Чтобы убедиться, что можно будет восстановить данные после аварии, настройте процедуру перемещения ленточных томов из пула хранения копий в расположение вне площадки. Инструкции смотрите в разделе Подготовка к аварии и восстановление после аварии с использованием DRM.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
Информация, связанная с данной:
DEFINE STGPOOL (определение тома в пуле хранения)

Защита приложений и компьютеров

Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы.

- Добавление клиентов
  После успешной настройки сервера IBM Spectrum Protect установите и сконфигурируйте программу клиента, чтобы начать резервное копирование данных.

Конфигурирование перемещения данных в режиме без сети;

Можно сконфигурировать клиент и сервер IBM Spectrum Protect так, чтобы клиент мог переместить данные через агент хранения непосредственно в хранилище в сети хранения данных (SAN). Эта функция называется перемещением данных в режиме без локальной сети, и она предоставляется IBM Spectrum Protect for SAN product.

Процедура

Чтобы сконфигурировать перемещение данных без локальной сети, выполните следующие шаги. Дополнительную информацию смотрите в документации к IBM Spectrum Protect for SAN.

1. Проверьте сетевое соединение.
2. Установите связь между клиентом, агентом хранения и сервером.
3. Установите и сконфигурируйте программное обеспечение систем клиентов.
4. Сконфигурируйте на сервере устройства, к которым будет обращаться агент хранения.
5. Сконфигурируйте политики перемещения данных в режиме без локальной сети IBM Spectrum Protect для клиента.
6. При работе с совместно используемой системой хранения FILE установите и сконфигурируйте IBM® TotalStorage SAN File System или IBM Spectrum Scale.
   Операционные системы WindowsОграничение: Если том IBM Spectrum Scale сформатирован сервером AIX, система Windows использует для передачи данных TCP/IP, а не сеть хранения данных (storage area network, SAN).
7. Определите пути от агента хранения к накопителям.
8. Запустите агент хранения и проверьте конфигурацию без локальной сети.

Дальнейшие действия

Для упрощения настройки ресурсов локальной сети и сети хранения можно контролировать пути перемещения данных для клиентов с функцией перемещения данных в режиме без локальной сети. Чтобы управлять путем, используйте команду UPDATE NODE. Для каждого клиента можно выбрать для операций чтения и записи данных один из следующих

параметров. Задайте операции чтения данных, используя параметр DATAREADPATH, и операции записи данных, используя параметр DATAWRITEPATH. Это необязательный параметр. Значение по умолчанию - ANY.

LAN (только путь в локальной сети)
Задайте значение LAN, если выполняется любое из следующих условий:

- Вы хотите произвести резервное копирования или восстановление небольшого объема данных.
- У клиента нет соединений SAN.

LANFREE (только путь без локальной сети)
Задайте значение LANFREE, если клиент и сервер находится в одной и той же SAN и если выполняется любое из следующих условий:

- Вы хотите произвести резервное копирования или восстановление большого объема данных.
- Вы хотите выгрузить нагрузку по серверной обработке на клиент.
- Вы хотите снять конфликты локальной сети.

ANY (любой доступный путь)
Если доступен путь без локальной сети, то он будет использован. Если путь без локальной сети недоступен, данные будут перемещены через локальную сеть.

- Проверка конфигурации для использования режима без локальной сети
  После конфигурирования клиента IBM Spectrum Protect для перемещения данных в режиме без локальной сети можно проверить конфигурацию и определения сервера при помощи команды VALIDATE LANFREE.

Методы шифрования лент

Выбор используемого метода шифрования зависит от планируемого способа управления данными.

Крайне важно защитать данные клиента, особенно, если эти данные - конфиденциальные. Чтобы гарантировать защиту данных на томах на площадке и вне площадки, существует технология шифрования лент IBM.

Ленточная технология IBM поддерживает разные методы шифрования накопителей для следующих устройств:

- IBM 3592 поколений 2 и 3
- IBM Linear Tape-Open (LTO) поколений 4 и 5

Методы шифрования накопителей, которые можно использовать в сочетании с IBM Spectrum Protect, конфигурируются на аппаратном уровне. IBM Spectrum Protect не может ни задать, ни изменить метод шифрования, используемый в аппаратной конфигурации. Если оборудование настроено для метода приложений, IBM Spectrum Protect может включить или выключить шифрование в зависимости от значения DRIVEENCRYPTION для класса устройств.

Чтобы зашифровать все данные в отдельной логической библиотеке или зашифровать данные более чем на одном томе пула хранения, используйте метод Библиотека или Система. Если менеджер ключей шифрования настроен для совместного использования ключей, методы Библиотека и Система могут совместно использовать ключ шифрования, обеспечивая взаимозаменяемость этих двух методов. IBM Spectrum Protect не может совместно использовать или отдельно использовать ключи шифрования из метода Приложение и либо метода шифрования Библиотека, либо либо метода шифрования Система.

Табл. 1. Методы шифрования

Метод шифрования	**Описание**

Метод шифрования	Описание
Шифрование на уровне приложения	Используя шифрование, управляемое приложением, можно создать отдельные пулы хранения, содержащие только зашифрованные тома. Таким образом можно использовать иерархии и политики пулов хранения для управления способом шифрования данных. Ключами шифрования управляет приложение, в данном случае, IBM Spectrum Protect. IBM Spectrum Protect генерирует и хранит ключи в базе данных сервера. Шифруются данные во время операций записи, когда ключ шифрования передается с сервера на накопитель. Для операций чтения данные расшифровываются. Чтобы зашифровать тома пула хранения и устранить часть обработки шифрования в системе, включите метод Приложение. Используйте шифрование, управляемое приложением, только для томов пула хранения. Другие тома, например, ленты с наборами резервных копий, жкспортируемые тома и резервные копии базы данных, не шифруются с использованием метода Приложение. Требование: Если включено шифрование приложений, вы должны особо тщательно подходить к защите резервных копий базы данных, так как ключи шифрования, используемые для шифрования и расшифровки данных, хранятся в базе данных сервера. Для восстановления данных необходимо иметь правильную резервную копию базы данных и соответствующие ключи шифрования для доступа к информации. Во избежание потери или кражи данных следует часто создавать резервные копии базы данных и обеспечивать их безопасность. Любой пользователь, имеющий доступ к резервной копии базы данных и ключам шифрования, получит доступ к вашим данным.
Шифрование на уровне библиотеки	Используя управляемое библиотекой шифрование, можно управлять тем, какие тома будут зашифрованы с использованием их серийных номеров. Можно задать диапазон или набор томов, которые необходимо шифровать. Ключами шифрования управляет библиотека. Они хранятся в менеджере ключей шифрования и передаются на накопитель. Если вы настроите оборудование для использования шифрования, управляемого библиотекой, вы сможете использовать этот метод, введя команду DEFINE DEVCLASS и задав параметр DRIVEENCRYPTION=ALLOW. Ограничение: Шифрование IBM LTO-4 и новее поддерживают только некоторые библиотеки IBM. Дополнительные сведения смотрите в разделе Конфигурирование шифрования ленточных накопителей.
Шифрование на уровне системы	Управляемое системой шифрование доступно только в операционной системе AIX®. Ключами шифрования, которые передаются накопителю, управляет драйвер устройства или операционная система, а хранятся они в менеджере ключей шифрования. Если оборудование настроено для использования системного шифрования, вы сможете использовать этот метод, введя команду DEFINE DEVCLASS и задав параметр DRIVEENCRYPTION=ALLOW.

Чтобы определить, зашифрован ли том и какой метод использовался, введите команду QUERY VOLUME и задайте параметр FORMAT=DETAILED.

- Конфигурирование шифрования ленточных накопителей
  Шифрование накопителей можно использовать для защиты лент, содержащих важные или конфиденциальные данные (например, лент с конфиденциальной финансовой информацией). Шифрование накопителей может быть полезно, если вы перемещаете ленты из среды сервера IBM Spectrum Protect в расположение на площадке или вне площадки.

Управление операциями ленточного хранения

В определениях классов устройств для ленточных устройств есть параметры, позволяющие управлять операциями хранения.

- Как IBM Spectrum Protect заполняет тома
  Команда DEFINE DEVCLASS имеет необязательный параметр ESTCAPACITY, который показывает примерную емкость томов с последовательным доступом, связанных с классом устройства. В IBM Spectrum Protect примерная емкость томов используется для оценки емкости пула хранения данных и процента используемого пространства.
- Указание оценочной емкости ленточных томов
  В IBM Spectrum Protect примерная емкость используется также для определения времени начала высвобождения томов пула хранения.
- Указание формата записей для ленточных носителей
  Можно задать формат записи, используемый IBM Spectrum Protect для записи данных на ленточный носитель. Если вы собираетесь использовать в библиотеке разные поколения накопителей или разные типы накопителей, вы должны задать формат записи для каждого поколения накопителей и для каждого типа накопителей. Тогда сервер сможет различать поколения накопителей и типы накопителей.
- Как связать объекты библиотеки с классами устройств
  Библиотека содержит накопители, которые можно использовать для монтирования тома. С классом устройства может быть связана только одна библиотека. Тем не менее, несколько классов устройств могут обращаться к одной библиотеке.
- Управление операциями монтирования носителей для ленточных и оптических устройств
  Используя определения классов устройств, можно управлять числом смонтированных томов, интервалом времени, в течение которого том остается смонтированным, а также тем, сколько времени сервер IBM Spectrum Protect будет ждать, чтобы накопитель стал доступен.
- Прерывание операций
  Сервер может прервать операции клиента или сервера для более приоритетной задачи, если точка монтирования используется, а других доступных точек нет, или если требуется доступ к конкретному тому. Когда операция прерывается, она отменяется.
- Влияние изменений устройств в SAN
  Среда SAN может сильно измениться из-за изменения устройств или кабелей. Динамический характер SAN данных может привести к ошибкам или непредвиденному поведению статических определений.
-  Операционные системы WindowsВывод сведений об устройстве
  Можно посмотреть сведения об устройствах, соединенных с сервером, используя утилиту информации об устройствах (tsmdlst).
- Носители с однократной записью и многократным чтением (WORM)
  Носители с однократной записью и многократным чтением (Write-Once, Read-Many - WORM) помогают предотвратить случайное или намеренное удаление критически важных данных. Однако в IBM Spectrum Protect существует ряд ограничений и рекомендаций, которым нужно следовать при использовании носителей WORM.
-  Операционные системы WindowsУстранение ошибок устройств
  Можно произвести поиск и устранение ошибок, возникших при конфигурировании или использовании устройств с IBM Spectrum Protect.

Как IBM Spectrum Protect заполняет тома

Команда DEFINE DEVCLASS имеет необязательный параметр ESTCAPACITY, который показывает примерную емкость томов с последовательным доступом, связанных с классом устройства. В IBM Spectrum Protect примерная емкость томов используется для оценки емкости пула хранения данных и процента используемого пространства.

Если параметр ESTCAPACITY не задан, IBM Spectrum Protect использует значение по умолчанию, основываясь на формате записи, который указан для класса устройства (параметр FORMAT=).

Если указать примерную емкость, которая превышает фактическую емкость тома в классе устройства, IBM Spectrum Protect обновит примерную емкость тома при его заполнении. Когда IBM Spectrum Protect заполнит том полностью, произойдет обновление емкости в соответствии с объемом, записанным в том.

Можно принять стандартное значение примерной емкости для класса устройства или явно указать примерную емкость. Точное значение примерной емкости не требуется, но рекомендуется. В IBM Spectrum Protect примерная емкость томов используется для оценки емкости пула хранения данных и процента используемого пространства. Примерную емкость может понадобиться изменить в следующих случаях:

- Примерная емкость по умолчанию неточна из-за сжатия данных.
- Используются тома нестандартного размера.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Указание оценочной емкости ленточных томов

В IBM Spectrum Protect примерная емкость используется также для определения времени начала высвобождения томов пула хранения.

Об этой задаче

Для классов ленточных устройств выбранные сервером значения по умолчанию зависят от формата записи, используемого при записи данных в том. Можно принять стандартное значение для типа устройств или указать собственное значение.

Чтобы задать примерную емкость ленточных томов, используйте параметр ESTCAPACITY при создании или обновлении определения класса устройств.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Указание формата записей для ленточных носителей

Можно задать формат записи, используемый IBM Spectrum Protect для записи данных на ленточный носитель. Если вы собираетесь использовать в библиотеке разные поколения накопителей или разные типы накопителей, вы должны задать формат записи для каждого поколения накопителей и для каждого типа накопителей. Тогда сервер сможет различать поколения накопителей и типы накопителей.

Об этой задаче

Чтобы задать формат записи, используйте параметр FORMAT при создании или обновлении определения класса устройств.

Если формат всех накопителей, связанных с этим классом устройства, одинаков, укажите FORMAT=DRIVE. На сервере выбирается самый высокий формат, поддерживаемый накопителем, на котором смонтирован том.

Если некоторые накопители, связанные с классом устройств, поддерживают формат более плотной записи, чем другие, и укажите формат, совместимый со всеми накопителями.

Если в одной библиотеке SCSI есть накопители, основанные на разных технологиях ленточных устройств (например, DLT и LTO Ultrium), задайте уникальное значение параметра FORMAT для каждого определения класса устройств.

Пример конфигурирования смотрите в разделе Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей.

Формат записи, который сервер использует для тома, выбирается при первой записи данных на том. Обновление параметра FORMAT не влияет на носители, которые уже содержат информацию, до тех пор, пока эти носители не будут

перезаписаны сначала. Этот процесс может происходить после того, как том освобожден или удален, или после того, как все данные на томе устареют.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Как связать объекты библиотеки с классами устройств

Библиотека содержит накопители, которые можно использовать для монтирования тома. С классом устройства может быть связана только одна библиотека. Тем не менее, несколько классов устройств могут обращаться к одной библиотеке.

Об этой задаче

Чтобы связать класс устройств с библиотекой, используйте параметр LIBRARY при создании или обновлении определения класса устройств.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Управление операциями монтирования носителей для ленточных и оптических устройств

Используя определения классов устройств, можно управлять числом смонтированных томов, интервалом времени, в течение которого том остается смонтированным, а также тем, сколько времени сервер IBM Spectrum Protect будет ждать, чтобы накопитель стал доступен.

- Управление числом одновременно смонтированных томов
  Задавая предел монтирования для класса устройств, вы должны учесть, сколько устройств хранения связано с вашей системой. Также следует учесть, используется ли функция одновременной записи, связываете ли вы несколько классов устройств с одной библиотекой, а также то, сколько процессов выполняются одновременно.
- Управление интервалом времени, в течение которого том остается смонтированным
  Можно управлять интервалом времени, в течение которого смонтированный том останется смонтированным после выполнения последней операции ввода-вывода. Если том часто используется, можно улучшить его производительность, установив большую задержку размонтирования, чтобы избежать ненужных операций монтирования и размонтирования.
- Управление временем ожидания накопителя сервером
  Вы можете задать максимальное время (в минутах), в течение которого сервер IBM Spectrum Protect должен ждать, когда накопитель станет доступен для выполнения текущего запроса на монтирование.

Управление числом одновременно смонтированных томов

Задавая предел монтирования для класса устройств, вы должны учесть, сколько устройств хранения связано с вашей системой. Также следует учесть, используется ли функция одновременной записи, связываете ли вы несколько классов устройств с одной библиотекой, а также то, сколько процессов выполняются одновременно.

Об этой задаче

При выборе лимита монтирования класса устройств учтите следующее:

- Сколько устройств хранения подключено к вашей системе?

  Не указывайте значение лимита монтирования, превышающее количество связанных доступных накопителей в вашей системе. Если сервер пытается монтировать столько же томов, сколько задано лимитом монтирования, а больше для нужного тома нет доступных накопителей, происходит ошибка и сеанс клиента может быть завершен. (Это ограничение не относится к случаю, когда указан параметр DRIVES.)

Если у вас ресурсы библиотеки совместно используются в SAN разными серверами IBM Spectrum Protect, вы должны ограничить число ленточных накопителей, которые клиент библиотеки может использовать за один раз. Чтобы разрешить нескольким серверам клиентов библиотеки использовать библиотеку одновременно, задайте параметр MOUNTLIMIT, когда будете задавать или обновлять класс устройств на клиенте библиотеки. Дополнительную информацию о конфигурировании совместного использования библиотек смотрите в разделе Конфигурирование совместного использования библиотеки.

- Используется ли функция одновременной записи в первичных пулах хранения, пулах хранения копий и пулах активных данных?

  Задайте лимит монтирования, обеспечивающий достаточно точек монтирования для поддержки одновременной записи в первичный пул хранения и все связанные с ним пулы хранения копий и пулы активных данных.

- Связываете ли вы несколько классов устройств с одной библиотекой?

  Класс устройства, связанный с библиотекой, может использовать любой накопитель из библиотеки, совместимый с классом и типом устройства. Поскольку с библиотекой можно связать насколько классов устройств, один накопитель в библиотеке может использоваться несколькими классами устройств. IBM Spectrum Protect гарантирует, что две операции не смогут одновременно использовать один и тот же накопитель, используя два разных класса устройств.

- Сколько процессов IBM Spectrum Protect необходимо запускать одновременно с использованием устройств этого класса?

  IBM Spectrum Protect автоматически отменяет некоторые процессы, чтобы запустить другие, с более высоким приоритетом. Если на сервере задействованы все доступные накопители данного класса устройств для выполнения процессов с более высоким приоритетом, процессы с более низким приоритетом должны ожидать, пока накопитель не будет доступен. Например, IBM Spectrum Protect отменяет для клиента процесс, когда производится непосредственное резервное копирование на ленту, если накопитель нужен для процесса переноса сервера или высвобождения ленты. IBM Spectrum Protect отменяет процесс высвобождения ленты, если накопитель нужен для операции восстановления клиента. Дополнительную информацию смотрите в разделе Прерывание операций.

  Если процессы часто отменяются другими процессами, возможно, следует сделать больше накопителей доступными для использования в IBM Spectrum Protect. Можно также изменить расписание операций, чтобы уменьшить нагрузку на накопители.

  Это замечание также относится к функции одновременной записи. Чтобы обеспечить успешное выполнение операции одновременной записи, надо иметь достаточное число накопителей.

  Чтобы задать максимальное число томов, которые можно одновременно смонтировать, используйте параметр MOUNTLIMIT при создании или обновлении определения класса устройств.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Управление интервалом времени, в течение которого том остается смонтированным

Можно управлять интервалом времени, в течение которого смонтированный том останется смонтированным после выполнения последней операции ввода-вывода. Если том часто используется, можно улучшить его производительность, установив большую задержку размонтирования, чтобы избежать ненужных операций монтирования и размонтирования.

Об этой задаче

Если операции монтирования выполняются вручную оператором, вам, возможно, стоит задать большую задержку размонтирования. Например, если один оператор обслуживает систему в выходные дни, задайте большую задержку размонтирования, чтобы система не спрашивала оператора каждые несколько минут, следует ли монтировать тома.

Чтобы управлять интервалом времени, в течение которого смонтированный том останется смонтированным, используйте параметр MOUNTRETENTION при создании или обновлении определения класса устройств. Например, если значение

задержки размонтирования равно 60 и смонтированный том простаивает в течение 60 минут, то сервер размонтирует том.

Если IBM Spectrum Protect монтирует том, накопитель выделяется для IBM Spectrum Protect и не может использоваться в других целях. Если требуется освободить накопитель для других целей, можно отменить операции IBM Spectrum Protect, в которых используется накопитель, а затем размонтировать том. Например, можно отменить операцию перенастройки сервера или резервного копирования. Информацию о том, как отменить процессы и размонтировать тома, смотрите в разделе Управление серверными запросами на тома.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Управление временем ожидания накопителя сервером

Вы можете задать максимальное время (в минутах), в течение которого сервер IBM Spectrum Protect должен ждать, когда накопитель станет доступен для выполнения текущего запроса на монтирование.

Об этой задаче

Для управления временем ожидания доступности накопителя по запросу монтирования используйте параметр MOUNTWAIT при определении или изменении класса устройств.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Прерывание операций

Сервер может прервать операции клиента или сервера для более приоритетной задачи, если точка монтирования используется, а других доступных точек нет, или если требуется доступ к конкретному тому. Когда операция прерывается, она отменяется.

Для просмотра состояния тома для точки монтирования, можно использовать команду QUERY MOUNT.

По умолчанию прерывание для сервера включено. Чтобы запретить прерывание, задайте опцию NOPREEMPT в файле опций сервера. Если вы зададите эту опцию, единственными операциями, которым разрешено прерывать другие операции, останутся команда BACKUP DB и команды экспорта и импорта.

- Приоритетное прерывание точки монтирования
  Если для операции с высоким приоритетом требуется точка монтирования в конкретном классе устройства, а все точки монтирования в этом классе в настоящее время используются, операция с высоким приоритетом может перехватить точку монтирования у операции с низким приоритетом.
- Приоритетное прерывание доступа к тому
  Если для операции с высоким приоритетом требуется доступ к конкретному тому, а этот том в настоящее время используется, операция с высоким приоритетом может прервать операцию с низким приоритетом для этого тома.

Ссылки, связанные с данной:
BACKUP DB (Выполнить резервное копирование базы данных)
QUERY MOUNT (Вывод сведений о смонтированных томах с последовательным доступом)

Приоритетное прерывание точки монтирования

Если для операции с высоким приоритетом требуется точка монтирования в конкретном классе устройства, а все точки монтирования в этом классе в настоящее время используются, операция с высоким приоритетом может перехватить точку монтирования у операции с низким приоритетом.

Точки монтирования могут быть перехвачены только в тех случаях, когда совпадает класс устройства у перехватывающей операции и у той операции, которая прерывается.

Следующие операции высокого приоритета могут прервать другие операции для доступа к точке монтирования.

- Операции резервного копирования базы данных
- Операции получения, восстановления или возврата HSM, инициированные клиентами
- Операции восстановления с использованием удаленного средства перемещения данных
- Операции экспорта
- Операции импорта
- Операции генерирования набора резервных копий

Следующие операции на сервере не могут прервать другие операции или сами быть прерванными:

- Аудит тома
- Восстановление данных из пула копий или активных данных
- Подготовка файла плана восстановления
- Сохранение данных с помощью удаленного переноса данных

Могут быть прерваны следующие операции, перечисленные в порядке приоритета, от наибольшего приоритета к наименьшему. Сервер выбирает для прерывания операции с наименьшим приоритетом, например, идентификацию дубликатов.

- Репликация узлов
- Резервное копирование данных в пул хранения копий
- Копирование активных данных в пул активных данных
- Перемещение данных в том пула хранения
- Перенос данных с диска на носитель с последовательным доступом
- Перенос данных с одного носителя с последовательным доступом на другой
- Операции резервного копирования, архивирования и переноса HSM, инициированные клиентами
- Высвобождение томов в пуле хранения с последовательным доступом
- Обнаружить дубликаты

Приоритетное прерывание доступа к тому

Если для операции с высоким приоритетом требуется доступ к конкретному тому, а этот том в настоящее время используется, операция с высоким приоритетом может прервать операцию с низким приоритетом для этого тома.

Например, если для запроса на восстановление требуется доступ к тому, который занят операцией высвобождения пространства, и накопитель доступен, операция высвобождения прерывается.

Следующие операции с высоким приоритетом могут прервать операции для доступа к конкретному тому:

- Операции резервного копирования базы данных
- Операции получения, восстановления или возврата HSM, инициированные клиентами
- Операции восстановления с использованием удаленного средства перемещения данных
- Операции экспорта
- Операции импорта
- Операции генерирования набора резервных копий

Следующие операции не могут прервать другие операции или сами быть прерванными:

- Аудит тома
- Восстановление данных из пула копий или активных данных
- Подготовка плана восстановления
- Сохранение данных с помощью удаленного переноса данных

Могут быть прерваны следующие операции, перечисленные в порядке приоритета, от наибольшего приоритета к наименьшему. Сервер выбирает для прерывания операции с наименьшим приоритетом, например, идентификацию дуюликатов.

- Репликация узлов
- Резервное копирование данных в пул хранения копий
- Копирование активных данных в пул активных данных
- Перемещение данных в том пула хранения
- Перенос данных с диска на носитель с последовательным доступом
- Перенос данных с одного носителя с последовательным доступом на другой

- Операции резервного копирования, архивирования и переноса HSM, инициированные клиентом
- Высвобождение томов в пуле хранения с последовательным доступом
- Обнаружить дубликаты

Влияние изменений устройств в SAN

Среда SAN может сильно измениться из-за изменения устройств или кабелей. Динамический характер SAN данных может привести к ошибкам или непредвиденному поведению статических определений.

ID устройств, назначенные сетью хранения данных и известные серверу или агенту хранения, могут быть изменены из-за сбросов шины или других изменений среды. Например, сервер может распознать устройство X как *rmt0* (в AIX) на основе исходной спецификации пути на ссервере и исходной конфигурации локальной сети. Однако некоторые события в SAN, например, добавление нового устройства Y, приводят к назначению *rmt1* устройству X. При попытке сервера получить доступ к устройству X с использованием *rmt0* либо доступ завершится неудачно, либо будет осуществлен доступ не к тому устройству назначения. Сервер попытается выполнить восстановление после внесения изменений в устройства в SAN, используя серийные номера устройств для подтверждения идентичности устройств, к которым он обращается.

При определении носителя или библиотеки у вас есть опция указания серийного номера для этого устройства. Если при определении устройства серийный номер не был указан, сервер получит его во время определения пути к устройству. В любом случае в базе данных сервера будет серийный номер устройства, который он сможет использовать для подтверждения идентичности устройства для операции.

При использовании накопителей и библиотек в сети SAN сервер пытается проверить, является ли используемое устройство нужным устройством. Сервер устанавливает связь с устройством с помощью имени устройства и указанного пути. Затем сервер запрашивает серийный номер устройства и сравнивает его с серийным номером устройства в базе данных.

Если серийный номер не совпадает, сервер начинает процесс поиска устройств в SAN, пытаясь найти устройство с совпадающим серийным номером. Если сервер находит устройство с нужным серийным номером, он исправляет определение пути в базе данных сервера, обновив имя устройства, указанное в пути. Сервер выдает сообщение с информацией об изменении, произведенном в устройстве. Затем сервер приступает к использованию устройства.

Чтобы определить, когда изменения устройства в SAN влияют на сервер IBM Spectrum Protect, можно отслеживать сообщения в журнале операций. С серийными номерами связаны следующие сообщения:

- ANR8952 — ANR8958;
- ANR8961 - ANR8968;
- ANR8974 - ANR8975.

Ограничения: Некоторые устройства не могут сообщить свои серийные номера прикладным программам, таким как сервер IBM Spectrum Protect. Если сервер не может получить серийный номер с устройства, сервер не сможет помочь системе восстановиться после изменения расположения устройства в SAN.
Операционные системы Windows

Вывод сведений об устройстве

Можно посмотреть сведения об устройствах, соединенных с сервером, используя утилиту информации об устройствах (tsmdlst).

Прежде чем начать

- Убедитесь, что у вас установлен API HBA (адаптер шины хоста). API HBA требуется, чтобы запустить утилиту информации об устройствах.
- Убедитесь, что у вас установлен и сконфигурирован драйвер ленточных устройств.

Процедура

1. В командной строке перейдите в подкаталог `server` каталога установки сервера, например, C:\Program Files\Tivoli\TSM\server.
2. Запустите исполняемый файл tsmdlst.exe.

Ссылки, связанные с данной:

QUERY SAN (Запросить список устройств в сети хранения данных)
tsmdlst (Вывод информации об устройствах)

Носители с однократной записью и многократным чтением (WORM)

Носители с однократной записью и многократным чтением (Write-Once, Read-Many - WORM) помогают предотвратить случайное или намеренное удаление критически важных данных. Однако в IBM Spectrum Protect существует ряд ограничений и рекомендаций, которым нужно следовать при использовании носителей WORM.

С IBM Spectrum Protect можно использовать следующие типы носителей WORM:

- IBM® 3592, все поддерживаемые поколения
- IBMLTO-3 и все поддерживаемые поколения
- HP LTO-3 и все поддерживаемые поколения
- Quantum LTO-3 и все поддерживаемые поколения
- Quantum SDLT 600, Quantum DLT V4 и Quantum DLT S4.
- StorageTek VolSafe;
- Sony AIT50 и AIT100;

Советы:

- Пул хранения может состоять либо из носителей WORM, либо из носителей RW, но не из носителей обоих типов.
- Чтобы не тратить напрасно ленту после выполнения операции восстановления или импорта, не используйте ленты WORM для операций резервного копирования или экспорта базы данных.

- Накопители, поддерживающие WORM
  Чтобы можно было использовать в библиотеке носители WORM, все накопители библиотеки должны поддерживать WORM. Монтирование не удастся, если картридж WORM будет смонтирован в накопитель для чтения и записи (RW).
- Активация носителей WORM
  Тип носителей WORM определяет, нужно ли читать метку носителя при активации носителя.
- Ограничения, касающиеся носителей WORM
  Использовать носители WORM с заранее присвоенной меткой в сочетании с классом устройств LTO или ECARTRIDGE нельзя.
- Ошибки монтирования при использовании носителей класса WORM
  Если ленточный носитель WORM загрузить в накопитель для устройств класса RW (чтение и запись), то монтирование завершится неудачно. Аналогичным образом, если ленточный носитель RW загрузить в накопитель для устройств класса WORM, то монтирование завершится неудачно.
- Изменение меток носителей WORM
  Если картридж WORM содержит данные, изменять его метку нельзя. Это касается картриджей Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM и IBM 3592. Метку на томе VolSafe можно перезаписать только один раз и только при условии, что том не содержит используемых, удаленных или просроченных данных.
- Удаление закрытых томов WORM из библиотеки
  Если над томом WORM совершаются действия (например, удаление промежутков между файлами), и сервер не отмечает том как заполненный, то этому тому возвращается состояние чистого. Если том WORM, не отмеченный как заполненный, удалить из пула хранения, то он останется закрытым. Чтобы удалить закрытый том WORM из библиотеки, необходимо выполнить команду CHECKOUT LIBVOLUME.
- Создание томов DLT WORM
  Тома DLT WORM можно преобразовать из томов RW (чтение/запись).
- Поддержка коротких и обычных лент 3592 WORM
  IBM Spectrum Protect поддерживает как короткие, так и обычные ленты 3592 WORM. Для получения наилучших результатов их следует задавать в отдельных пулах хранения
- Как запросить в классе устройств информацию о значении параметра WORM
  Значение параметра WORM для класса устройств можно определить, введя команду QUERY DEVCLASS. Выходная информация будет содержать поле "WORM", в котором будет находиться значение YES (Да) или NO (Нет).

Накопители, поддерживающие WORM

Чтобы можно было использовать в библиотеке носители WORM, все накопители библиотеки должны поддерживать WORM. Монтирование не удастся, если картридж WORM будет смонтирован в накопитель для чтения и записи (RW).

Однако накопитель, поддерживающий WORM, можно использовать в качестве RW-накопителя, если установить для параметра WORM в классе устройства значение NO. Библиотека любого типа может содержать носители как WORM, так и

RW, если во *всех* устройствах активирован WORM. Единственным исключением из этого правила являются библиотеки, подключенные к NAS, в которых использование ленточных носителей WORM невозможно.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
Информация, связанная с данной:
UPDATE DEVCLASS (изменение класса устройства)

Активация носителей WORM

Тип носителей WORM определяет, нужно ли читать метку носителя при активации носителя.

Чейнджеры носителей библиотек не способны распознать разницу между стандартным ленточным носителем RW (чтение/запись) и следующими типами ленточных носителей WORM:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Чтобы определить тип используемого носителя WORM, том необходимо загрузить в накопитель. Поэтому при регистрации томов WORM одного из этих типов нужно указывать опцию CHECKLABEL=YES в команде CHECKIN LIBVOLUME.

Библиотечные чейнджеры IBM® 3592, которые поддерживают носители WORM, могут определять, является ли том носителем WORM, без загрузки тома в накопитель. Указывать CHECKLABEL=YES не нужно. Следует выяснить у поставщика оборудования, обеспечивают ли накопители и библиотеки 3592 необходимую поддержку.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Ограничения, касающиеся носителей WORM

Использовать носители WORM с заранее присвоенной меткой в сочетании с классом устройств LTO или ECARTRIDGE нельзя.

Носители WORM нельзя использовать, если IBM Spectrum Protect задан как менеджер ключей шифрования накопителей для следующих накопителей:

- IBM® LTO-5, LTO-6 и новее
- HP LTO-5, LTO-6 и новее
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

Ошибки монтирования при использовании носителей класса WORM

Если ленточный носитель WORM загрузить в накопитель для устройств класса RW (чтение и запись), то монтирование завершится неудачно. Аналогичным образом, если ленточный носитель RW загрузить в накопитель для устройств класса WORM, то монтирование завершится неудачно.

Изменение меток носителей WORM

Если картридж WORM содержит данные, изменять его метку нельзя. Это касается картриджей Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM и IBM® 3592. Метку на томе VolSafe можно перезаписать только один раз и только при условии, что том не содержит используемых, удаленных или просроченных данных.

Вводите команду LABEL LIBVOLUME для каждого тома VolSafe только по одному разу. Защиту от изменения метки можно установить с помощью параметра OVERWRITE=NO команды LABEL LIBVOLUME.

Ссылки, связанные с данной:

LABEL LIBVOLUME (запись метки на том библиотеки)

Удаление закрытых томов WORM из библиотеки

Если над томом WORM совершаются действия (например, удаление промежутков между файлами), и сервер не отмечает том как заполненный, то этому тому возвращается состояние чистого. Если том WORM, не отмеченный как заполненный, удалить из пула хранения, то он останется закрытым. Чтобы удалить закрытый том WORM из библиотеки, необходимо выполнить команду CHECKOUT LIBVOLUME.

Ссылки, связанные с данной:
CHECKOUT LIBVOLUME (исключение тома хранения из библиотеки)

Создание томов DLT WORM

Тома DLT WORM можно преобразовать из томов RW (чтение/запись).

Чтобы обеспечить поддержку носителей WORM при работе с накопителями SDLT-600, DLT-V4 или DLT-S4, можно обновить эти накопители с использованием программно-аппаратного обеспечения V30 или более поздней версии, которое можно приобрести у Quantum. Можно также использовать программное обеспечение DLTIce для преобразования неформатированных томов RW или пустых томов в тома WORM.

В библиотеках SCSIсервер IBM Spectrum Protect автоматически создает чистые тома DLT WORM, когда не может найти никаких чистых томов WORM в перечне библиотеки. Сервер преобразует доступные неформатированные или пустые чистые тома RW, а также пустые закрытые тома RW, в чистые тома WORM. Сервер также меняет метки на вновь созданных томах WORM, используя информацию из меток существующих томов RW.

Поддержка коротких и обычных лент 3592 WORM

IBM Spectrum Protect поддерживает как короткие, так и обычные ленты 3592 WORM. Для получения наилучших результатов их следует задавать в отдельных пулах хранения

Как запросить в классе устройств информацию о значении параметра WORM

Значение параметра WORM для класса устройств можно определить, введя команду QUERY DEVCLASS. Выходная информация будет содержать поле "WORM", в котором будет находиться значение YES (Да) или NO (Нет).

Информация, связанная с данной:
Команда QUERY DEVCLASS (отображение информации об одном или нескольких классах устройств)
Операционные системы Windows

Устранение ошибок устройств

Можно произвести поиск и устранение ошибок, возникших при конфигурировании или использовании устройств с IBM Spectrum Protect.

Об этой задаче

Используйте Табл. 1 для поиска решения возникшей с устройством проблемы.

Табл. 1. Устранение проблем устройств

Симптом	Проблема	Решение

Симптом	Проблема	Решение
Конфликты с другими программами.	Продукту IBM Spectrum Protect требуется сеть хранения данных для совместного использования устройств.	Настроить сеть хранения данных. Внимание: Если несколько серверов IBM Spectrum Protect используют одно и то же устройство, возможна потеря данных. Задавайте или используйте устройство только с одним сервером IBM Spectrum Protect  Операционные системы AIX  Операционные системы LinuxДругие приложения могут получить доступ к устройствам IBM Spectrum Protect, используя ленточный драйвер SCSI.
Ошибка присвоения метки.	Устройство для присвоения метки томам нельзя использовать во время использования сервером устройства для выполнения других процессов.	Перезаписать существующие тома в пуле хранения нельзя. Вы должны устранить все аппаратные ошибки, прежде чем присваивать тому метку.
	Неправильная или неполная регистрация лицензии.	Зарегистрируйте приобретенную лицензию на поддержку устройств.
Конфликты между драйверами устройств.	IBM Spectrum Protect выводит сообщения об ошибках ввода-вывода при определении или использовании устройств с последовательным доступом.	Драйверы устройств Windows и драйверы, предоставляемые другими прикладными программами, могут конфликтовать с драйвером устройств IBM Spectrum Protect, если драйвер IBM Spectrum Protect не запущен первым. Чтобы проверить порядок запуска драйверов устройств системой, выполните следующие шаги: 1. Щелкните по значку Панель управления. 2. Щелкните по Устройства. Драйвера устройств и соответствующие типы запуска перечислены.
Ошибки ввода-вывода	Если вы попытаетесь задать или использовать ленточное устройство, могут возникнуть конфликты драйверов устройств. Драйверы устройств Windows и драйверы, предоставляемые другими прикладными программами, могут конфликтовать с драйвером устройств IBM Spectrum Protect, если он не запущен первым.	

Завершение реализации

После того, как решение IBM Spectrum Protect будет сконфигурировано и заработает, проверьте операции резервного копирования и настройте мониторинг, чтобы убедиться, что все нормально работает.

Процедура

1. Проверьте операции резервного копирования, чтобы убедиться, что ваши данные защищены, как вы и ожидали.

a. Выберите на странице Клиенты компонента Центр операций клиенты, для которых вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
b. На странице Серверы в компоненте Центр операций выберите сервер, для которого вы хотите производить резервное копирование базы данных. Щелкните по Резервное копирование и выполните инструкции в окне Резервное копирование базы данных.
c. Убедитесь, что резервное копирование выполнено без предупреждений или сообщений об ошибках.
Совет: Либо можно использовать графический интерфейс клиента резервного копирования и архивирования для резервного копирования данных клиента, и можно производить резервное копирование базы данных, вводя команду BACKUP DB из административной командной строки.

2. Настройте мониторинг для ваших решений, следуя инструкциям в разделе Мониторинг ленточного решения.

Мониторинг ленточного решения

После реализации решения IBM Spectrum Protect на основе ленты выполняйте мониторинг решения, чтобы убедиться, что оно работает правильно. Выполняя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.

Об этой задаче

Предпочтительный способ мониторинга решения заключается в использовании компонента Центр операций, который позволяет получить общее и подробное состояние системы в графическом пользовательском интерфейсе. Кроме того, можно сконфигурировать Центр операций для генерирования отчетов по электронной почте, в которых суммируется состояние системы.

Процедура

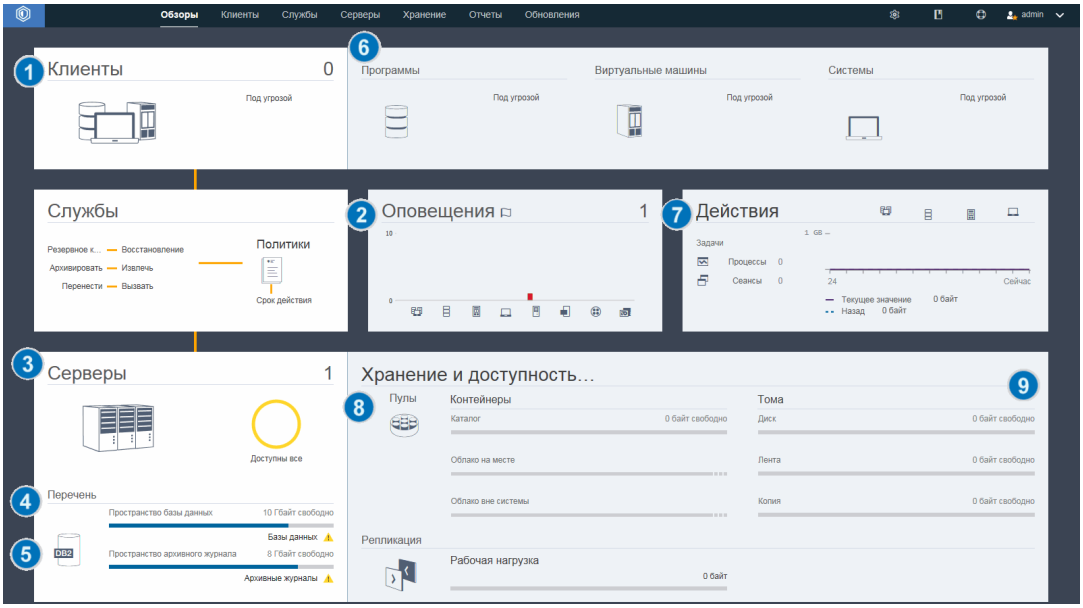
1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе Контрольный список ежедневного мониторинга.
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе Контрольный список периодического мониторинга.
3. Убедитесь, что ваша система удовлетворяет требованиям лицензирования. Инструкции смотрите в разделе Проверка соответствия лицензии.
4. Необязательно: Настройте отчеты по электронной почте с информацией о состоянии системы. Инструкции смотрите в разделе Состояние системы отслеживания с использованием отчетов по электронной почте.

Контрольный список ежедневного мониторинга

Чтобы убедиться, что вы выполняете ежедневные задачи мониторинга для своего решения IBM Spectrum Protect, ознакомьтесь с ежедневным контрольным списком для мониторинга.

Выполняйте ежедневные задачи мониторинга со страницы Обзор в компоненте Центр операций. Доступ к странице Обзор можно получить, открыв Центр операций и щелкнув по Обзоры.

На рисунке ниже показано расположение для завершения каждой операции.



Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

В следующей таблице перечислены ежедневные задачи мониторинга и представлены инструкции по выполнению каждой задачи.

Табл. 1. Задачи ежедневного мониторинга

Задача	**Основные процедуры**	**Дополнительные процедуры и диагностическая информация**

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
Наблюдайте за уведомлениями о защите, которые могут указывать на атаку программы-вымогателя.	Если потенциальная атака программы-вымогателя обнаружена в среде IBM Spectrum Protect, то будет показано уведомление о защите на переднем плане Центр операций. Дополнительную информацию можно получить, щелкнув по сообщению, чтобы открыть страницу Уведомления о защите.	На странице Уведомления о защите можно выполнить следующие действия: • Просмотр подробностей уведомления по клиентам. Ограничение: В Центр операций версии 8.1.5, уведомления доступны только для клиентов резервного копирования-архивирования. • Подтвердите уведомление защиты, выбрав его и щелкнув по Подтвердить. При подтверждении уведомления о защите в столбец Подтверждение на странице Уведомления о защите добавляется символ галочки для выбранного клиента. Стандарт, по которому подтверждается уведомление, определяется в вашей организации. Галочка может означать, что вы исследовали проблему и решили, что это - ложное положительное. Это также может означать, что проблема существует, и она решается. • Назначьте уведомление о защите администратору, выбрав уведомление о защите и нажав Назначить. Чтобы рассмотреть назначение, администратор должен зарегистрироваться в Центр операций и щелкнуть Обзоры > Защита. Если вы не уверены, что администратор регулярно отслеживает страницу Уведомления о защите, сообщите администратору о назначении. • Если уведомление - ложное положительное, то можно выбрать уведомление о защите и щелкните по Сброс. Уведомление о защите удалено. Хронологические данные, используемые для базовых сравнений с самой последней операцией резервного копирования, удаляются. С этого момента вычисляется новая базовая линия.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
1 Определите, подвергаются ли клиенты риску оказаться незащищенными из-за неудавшихся или пропущенных операций резервного копирования.	Чтобы проверить, находятся ли клиенты под угрозой, в области Клиенты найдите уведомление Под угрозой. Чтобы просмотреть сведения, щелкните по области Клиенты. Внимание: Если процент Под угрозой намного больше обычного, то это может указывать на атаку программы-вымогателя. Атака программы-вымогателя может привести к сбоям резервного копирования, тем самым создавая риск для клиентов. Например, если процент клиентов в опасности обычно между 5% и 10%, но процент увеличивается до 40% или 50%, то изучите причину этого. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете увидеть и проанализировать ошибку клиента и запланировать журналы, выполнив следующие шаги: 1. В таблице Клиенты выберите клиент и щелкните по Сведения. 2. Чтобы диагностировать проблему, щелкните по Диагноз.	В случае клиентов, у которых нет установленной службы управления клиентом, получите доступ к системе клиента, чтобы проверить журналы ошибок клиента.
2 Определите, нужно ли уделить внимание ошибкам клиента или сервера.	Чтобы определить серьезность всех оповещений, о которых было сообщено, установите указатель мыши на столбцы в области Оповещения.	Чтобы увидеть дополнительную информацию об оповещениях, выполните следующие шаги: 1. Щелкните по области Оповещения. 2. В таблице Оповещения выберите оповещение. 3. В панели Журнал операций просмотрите сообщения. В панели показаны связанные сообщения, созданные до и после возникновения выбранного оповещения.
3 Определите, доступны ли серверы, которыми управляет Центр операций, для предоставления клиентам служб по защите данных.	1. Чтобы проверить, находятся ли серверы под угрозой, в области Серверы найдите уведомление Недоступен. 2. Чтобы увидеть дополнительную информацию, щелкните по области Серверы. 3. Выберите сервер в таблице Серверы и щелкните по Сведения.	Совет: Если вы обнаружите проблему, связанную со свойствами сервера, обновите свойства сервера: 1. В таблице Серверы выберите сервер и щелкните по Сведения. 2. Чтобы обновить свойства сервера, щелкните по Свойства.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
4 Определите, доступно ли достаточно пространства для перечня сервера, состоящего из базы данных сервера, активного журнала и архивного журнала.	1. Щелкните по области Серверы. 2. В столбце Состояние в таблице проверьте состояние сервера и устраните все ошибки: ◦ Нормальное Для базы данных сервера, активного журнала и архивного журнала доступен достаточный объем пространства. ◦ Критическое Для базы данных сервера, активного журнала или архивного журнала недостаточно пространства. Нужно немедленно добавить пространство, иначе работа служб защиты данных, предоставляемых сервером, будет прервана. ◦ Предупреждение , В базе данных сервера, активном журнале или архивном журнале заканчивается пространство. Если это условие повторяется, то нужно добавить пространство. ◦ Недоступно Невозможно получить состояние. Убедитесь, что сервер работает и что в сети нет ошибок. Это состояние показывается также, если ID администратора мониторинга заблокирован или недоступен на сервере по другой причине. Значение этого ID - IBM-OC-имя_хаб-сервера. ◦ Неотслеживаемый Неотслеживаемые серверы заданы на хаб-сервере, но не сконфигурированы для управления компонентом Центр операций. Чтобы сконфигурировать не отслеживаемый сервер, выберите сервер и щелкните по Отслеживать подчиненный.	Можно также просмотреть связанные оповещения на странице Оповещения. Дополнительную информацию об устранении ошибок смотрите в разделе Устранение проблем сервера.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
5 Проверьте операции резервного копирования базы данных.	Чтобы определить, когда в последний раз производилось резервное копирование сервера, выполните следующие шаги: 1. Щелкните по области Серверы. 2. В таблице Серверы проверьте столбец Последнее резервное копирование базы данных.	Чтобы получить более подробную информацию об операциях резервного копирования, выполните следующие шаги: 1. В таблице Серверы выберите строку и щелкните по Сведения. 2. В области Резервное копирование БД установите указатель мыши на галочки, чтобы прочесть информацию об операциях резервного копирования. Если резервное копирование базы данных не производилось недавно (например, за последние 24 часа), вы можете запустить операцию резервного копирования: 1. На странице Обзор в компоненте Центр операций щелкните по области Серверы. 2. В таблице выберите сервер и щелкните по Резервное копирование. Чтобы определить, сконфигурирована ли база данных сервера для автоматических операций резервного копирования, выполните следующие шаги: 1. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY DB: `query db f=d` 3. В выходной информации проверьте значение в поле `Полное имя класса устройств`. Если класс устройства указан, это означает, что сервер сконфигурирован для автоматического резервного копирования базы данных.
6 Отслеживайте другие задачи по обслуживанию сервера. Задачи по обслуживанию сервера могут включать в себя выполнение расписаний административных команд, сценариев обслуживания и связанных команды.	Чтобы найти информацию о процессах, которые завершились неудачно из-за проблем на сервере, выполните следующие шаги: 1. Выберите Серверы > Обслуживание. 2. Чтобы получить двухнедельную хронологию процесса, смотрите столбец Хронология. 3. Чтобы получить больше информации о запланированном процессе, установите указатель мыши на переключателее, связанном с процессом.	Более подробную информацию о процессах мониторинга и устранении проблем смотрите в электронной справке компонента Центр операций.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
7 Убедиться, что объем данных, переданных на серверы и полученных с них, находится в ожидаемом диапазоне.	• Чтобы получить обзор операций за последние 24 часа, смотрите область Операции. • Чтобы сравнить активность за последние 24 часа с активностью за предыдущие 24 часа, смотрите показатели в областях Текущие и Предыдущие.	• Если на сервер было отправлено больше данных, чем вы ожидали, определите, какие клиенты создают резервные копии большего объема данных, и исследуйте причину. Возможно, что дедупликация данных на стороне клиента работает неправильно. Внимание: Если объем резервных данных значительно больше обычного, то это может указывать на атаку программы-вымогателя. Когда программа-вымогатель шифрует данные, система обнаруживает, что данные изменяются и что резервная копия создается для измененных данных. Тем самым тома резервного копирования становятся больше. Чтобы узнать, какие клиенты затронуты, выберите вкладки Приложения, Виртуальные или Системы. • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.
8 Убедитесь, что пулы хранения доступны для резервного копирования данных клиента.	1. Если в области Хранение и доступность данных указаны проблемы, щелкните по Пулы, чтобы ознакомиться со сведениями: ◦ Если показано состояние Критическое ⊗, это указывает на то, что в пуле хранения недостаточно доступного пространства или его состояние доступа - Недоступно. Внимание: Если состояние критическое, то изучите причину: ▪ Если скорость дедупликации данных в пуле хранения значительно снижается, то это может указывать на атаку программы-вымогателя. Во время атаки программы-вымогателя данные шифруются и не могут дедуплицироваться. Чтобы проверить скорость дедупликации данных, в таблице Пулы хранения проверьте значение в столбце Процент экономии. ▪ Если пул хранения неожиданно становится использован 100%, то это может указывать на атаку программы-	Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по Сведения.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
	вымогателя. Для проверки использования просмотрите значение в столбце Использованная емкость. Наведите мышь на значения, чтобы увидеть процент использованного и свободного пространства. ○ Если показано состояние Предупреждение ⚠, в пуле хранения заканчивается пространство или его состояние доступа - Только чтение. 2. Чтобы увидеть и используемое, свободное и общее пространство для выбранного пула хранения, установите указатель мыши над записями в столбце Использованная емкость.	

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
9 Убедитесь, что устройства хранения доступны для операций резервного копирования.	В области Хранение и доступность данных, в разделе Тома под столбцами емкости проверьте состояние, показанное рядом с элементом Устройства. Если для любого устройства показано состояние Критическое или Предупреждение, исследуйте проблему. Чтобы просмотреть сведения, щелкните по Устройства.	Ленточные устройства могут находиться в состоянии предупреждения или в критическом состоянии, если накопители недоступны. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. Ленточное устройство может также находиться в критическом состоянии, если библиотека отключена. В других столбцах таблицы Ленточные устройства показано состояние роботизации библиотеки, накопителей и путей. Чтобы устранить проблемы с ленточными устройствами, находящимися в критическом состоянии, можно перевести накопитель в отключенное состояние, если вы хотите использовать его для других операций, например, для обслуживания. Чтобы перевести накопитель в отключенное состояния, выполните следующие шаги: 1. На странице компонента Центр операций Хранение выберите Ленточные устройства. 2. Чтобы увидеть больше информации о ленточной библиотеке, выберите строку и щелкните по Сведения. 3. Чтобы перевести накопитель в отключенное состояния, выберите ленточный накопитель и щелкните по Отключено. В случае операций резервного копирования лент убедитесь, что доступно достаточное число чистых лент. Если вы не уверены, есть ли у вас достаточное число доступных чистых лент, откройте записную книжку с подробной информацией, чтобы узнать об использовании ленты и увидеть оценку доступности чистых лент. Чтобы открыть записную книжку с подробной информацией, выберите библиотеку в таблице и щелкните по Сведения.

Контрольный список периодического мониторинга

Чтобы убедиться, что операции осуществляются правильно, выполните задачи в периодическом контрольном списке мониторинга. Запланируйте периодические задачи достаточно часто, чтобы вы могли обнаружить потенциальные неполадки, прежде чем они вызовут проблемы.

Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

Табл. 1. Задачи периодического мониторинга

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте производительность системы.	Определите, сколько времени требуется для операций резервного копирования клиента: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Найдите сервер, связанный с клиентом. 2. Щелкните по Серверы. Выберите сервер и щелкните по Сведения. 3. Чтобы увидеть продолжительность выполненных задач за последние 24 часа, щелкните по Выполненные задачи. 4. Чтобы увидеть продолжительность задач, выполненных более 24 часов тому назад, используйте команду QUERY ACTLOG. Информацию об этой команде смотрите в разделе . 5. Если длительность операций резервного копирования клиента увеличивается при неясных причинах, исследуйте причину. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете диагностировать ошибки, влияющие на производительность, для клиента резервного копирования и архивирования, выполнив следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. 2. Выберите клиент резервного копирования и архивирования и щелкните по Сведения. 3. Чтобы получить журналы клиентов, щелкните по Диагностика.	Ограничьте время для операций резервного копирования клиента 8-12 часами. Убедитесь, что расписания клиентов не перекрываются с задачами по обслуживанию сервера. Инструкции по сокращению времени, которое затрачивает клиент на резервное копирование данных на сервер, смотрите в разделе https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.0/perf/c_bac_perf_opts.html. Ищите узкие места с точки зрения производительности. Инструкции смотрите в разделе Определение узких мест производительности. Информацию о выявлении и устранении других проблем, отрицательно влияющих на производительность, смотрите в разделе https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.0/perf/c_performance.html.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок

Убедитесь, что текущие файлы резервных копий для конфигурации устройств и информации о хронологии томов сохранены.	Получите доступ к расположениям хранения, чтобы убедиться, что файлы доступны. Предпочтительный метод заключается в том, чтобы сохранять файлы резервных копий в двум расположениях.
	Чтобы найти файлы хронологии томов и файлы конфигурации устройств, выполните следующие шаги:
	1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
	2. Чтобы найти файлы хронологии томов и конфигурации устройств, введите следующие команды:
	`query option volhistory`
	`query option devconfig`
	3. В выходной информации проверьте столбец Параметр опции, чтобы найти расположения файлов.
	Если произойдет бедствие, для восстановления базы данных сервера потребуется как файл хронологии томов, так и файл конфигурации устройств.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите, доступно ли достаточно пространства в каталоге для экземпляра сервера.	Убедитесь, что в каталоге для экземпляра сервера доступно хотя бы 50 ГБ свободного пространства. Выполните действие, подходящее для вашей операционной системы: •  Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -g` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра. •  Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -h` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра. •  В проводнике Windows щелкните правой кнопкой мыши по файловой системе и выберите Свойства. Проверьте информацию о емкости. Предпочтительное расположение каталога экземпляра зависит от операционной системы, в которой установлен сервер: •   /home/tsminst1/tsminst1 •  C:\tsminst1 Совет: Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Выявите неожиданную активность клиента.	Чтобы отслеживать операции клиента и определить, не превышает ли объем данных для томов ожидаемый объем, выполните следующие шаги: 1. На странице Обзор в компоненте Центр операций щелкните по области Клиенты. 2. Чтобы увидеть операции за посредние две недели, дважды щелкните по любому клиенту. 3. Чтобы узнать число байт, отправленных клиенту, щелкните по вкладке Свойства. 4. В области Последний сеанс проверьте строку Отправлено клиенту.	Когда вы дважды щелкнете по клиенту в таблице Клиенты, в области Операции за 2 недели будет показан объем данных, которые клиент каждый день отправлял на сервер. Регулярно проверяйте SQL-таблицу сводной информации о деятельности, содержащую статистические данные о клиентских сеансах. Чтобы сравнить текущие операции с предыдущими, воспользуйтесь оператором SQL SELECT. Если уровень операций существенно отличается от предыдущего, то это может указывать на атаку программы-вымогателя. Регулярно проверяйте журнал операций. Найдите сообщения ANE, указывающие, для скольких файлов созданы резервные копии и выполнена инспекция. Сравните текущие данные о скорости дедупликации с прежней скоростью. Если в созданной резервной копии необычно много файлов или уровень дедупликации данных неожиданно спадает до 0, то это может указывать на атаку программы-вымогателя

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте рост пула хранения с течением времени.	1. На странице Обзор в компоненте Центр операций щелкните по области Пулы. 2. Чтобы увидеть емкость, используемую за последние две недели, выберите пул и щелкните по Сведения.	Советы: • Чтобы задать период времени, который должен пройти, прежде чем из пула хранения каталогов-контейнеров или пула хранения облачных контейнеров будут удалены все дедуплицированные экстенты, после того как на них не появлялось никаких ссылок в перечне, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. 3. Задайте длительность в поле `Период задержки для повторного использования контейнера`. • Чтобы определить производительность дедупликации данных для пулов хранения каталогов-контейнеров и облачных контейнеров, используйте команду GENERATE DEDUPSTATS. • Чтобы просмотреть статистику дедупликации данных для пула хранения, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. Либо используйте команду QUERY EXTENTUPDATES, чтобы увидеть информацию об обновлениях экстентов данных в пулах хранения каталогов-контейнеров или облачных контейнеров. Выходная информация команды может помочь вам определить, на какие экстенты данных уже нет ссылок и какие из них подлежат удалению из системы. В выходной информации смотрите, какое число экстентов данных подлежит удалению из системы. Этот показатель напрямую коррелируется с объемом свободного пространства, которое доступно в пуле хранения контейнера. • Чтобы увидеть объем физического пространства, занятого файловым пространством после удаления экономии за счет дедупликации данных, используйте команду select * from occupancy. В выходной информации команды будет содержаться значение LOGICAL_MB. LOGICAL_MB - это объем, используемый этим файловым пространством.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте и обслуживайте ленточные устройства.	Отслеживайте в своей среде аппаратные ошибки на ленточных устройствах и ленточных библиотеках. Инструкции смотрите в разделе Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок. Отслеживайте совместимость носителей для предотвращения ошибок на ленточных устройствах. Инструкции смотрите в разделе Как избежать ошибок, связанных с несовместимостью носителей. Следите за сообщениями об очистке для ленточных накопителей. Инструкции смотрите в разделе Операции с чистящими картриджами.	
Оцените временные характеристики расписаний клиента. Убедитесь, что начальное и конечное время расписаний клиента не перекрывает задачи по обслуживанию сервера. Ограничьте время для операций резервного копирования клиента 8-12 часами.	Щелкните на странице Обзор в компоненте Центр операций по Клиенты > Расписания. В таблице Расписания в столбце Запуск показано сконфигурированное время запуска для запланированной операции. Чтобы увидеть, когда была запущена самая последняя операция, установите указатель мыши на значок часов.	Совет: Если операция клиента выполняется дольше, чем ожидается, вы можете получить сообщение с предупреждением. Сделайте следующее: 1. На странице обзора в компоненте Центр операций установите указатель мыши на Клиенты и щелкните по Расписания. 2. Выберите расписание и щелкните по Сведения. 3. Просмотрите сведения о расписании, щелкнув по синей стрелке рядом со строкой. 4. В поле Оповещение среды выполнения задайте время, когда будет выдано сообщение с предупреждением, если запланированная операция не будет выполнена. 5. Щелкните по Сохранить.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Оцените временные характеристики задач по обслуживанию. Убедитесь, что начальное и конечное время задач по обслуживанию не накладывается на расписания клиентов.	Щелкните на странице Обзор в компоненте Центр операций по Серверы > Обслуживание. В таблице Обслуживание проверьте информацию в столбце Время последнего выполнения. Чтобы увидеть, когда была запущена самая последняя задача по обслуживанию, установите указатель мыши на значок часов.	Предпочтительный метод заключается в том, что каждая задача по обслуживанию выполняется до ее завершения, прежде чем запустится следующая задача по обслуживанию. Примерами задач по обслуживанию являются признание перечня устаревшим, копирование пулов хранения, высвобождение пространства и резервное копирование базы данных. Совет: Если задача по обслуживанию выполняется слишком долго, измените начальное время или максимальное время работы. Сделайте следующее: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Чтобы изменить время запуска или максимальное время работы, введите команду UPDATE SCHEDULE. Информацию об этой команде смотрите в разделе UPDATE SCHEDULE (Изменить запланированное задание клиента).

- Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок
  Оповещения ленточных устройств генерируются ленточными и библиотечными устройствами и сообщают об аппаратных ошибках. Эти сообщения помогают определить проблемы, не связанные с сервером IBM Spectrum Protect.
- Как избежать ошибок, связанных с несовместимостью носителей
  Производя мониторинг и устраняя проблемы совместимости носителей, вы сможете предотвратить ошибки в решении на основе лент IBM Spectrum Protect. Новый накопитель может иметь ограниченную возможность использования форматов носителей, поддерживаемых накопителем предыдущей версии. Часто новый дисковод может считывать, но не записывать носители в старом формате.
- Операции с чистящими картриджами
  Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Ссылки, связанные с данной:
QUERY ACTLOG (Запросить информацию журнала операций)

Мониторинг оповещений ленточных устройств для выявления аппаратных ошибок

Оповещения ленточных устройств генерируются ленточными и библиотечными устройствами и сообщают об аппаратных ошибках. Эти сообщения помогают определить проблемы, не связанные с сервером IBM Spectrum Protect.

Об этой задаче

Создается страница журнала, которую можно получить в любой момент времени или в определенный момент, например, при размонтировании накопителя.

У сообщения с оповещением ленточных устройств может быть один из следующих уровней серьезности:

- Информационное (например, при попытке загрузить картридж неподдерживаемого типа)
- Предупреждение (например, если ожидается аппаратная ошибка);
- Критическое (например, если возникли неполадки с лентой и данные в опасности).

По умолчанию оповещения ленточных устройств отключены.

Процедура

- Чтобы включить сообщения с оповещениями ленточных устройств, введите команду SET TAPEALERTMSG и задайте значение ON: `set tapealertmsg on`
- Чтобы проверить, включены ли сообщения с оповещениями ленточных устройств, введите команду QUERY TAPEALERTMSG: `query tapealertmsg`

Как избежать ошибок, связанных с несовместимостью носителей

Производя мониторинг и устраняя проблемы совместимости носителей, вы сможете предотвратить ошибки в решении на основе лент IBM Spectrum Protect. Новый накопитель может иметь ограниченную возможность использования форматов носителей, поддерживаемых накопителем предыдущей версии. Часто новый дисковод может считывать, но не записывать носители в старом формате.

Об этой задаче

По умолчанию существующие тома, имеющие состояние `FILLING`, сохраняют это состояние после замены накопителя. В некоторых случаях для заполнения таких томов может возникнуть необходимость продолжать использование старого накопителя. При этом сохраняется возможность чтения и записи существующих томов до их освобождения. Если обновляются все накопители библиотеки, убедитесь, что форматы носителей поддерживаются новыми аппаратными средствами. Если с новыми накопителями планируется использовать не только новые носители, придется учитывать проблемы совместимости. Инструкции по переносу смотрите в разделе Перенос данных на обновленные накопители.

Чтобы использовать новый накопитель с носителями, которые он может считывать, но не записывать, введите команду UPDATE VOLUME, чтобы установить доступ к этим томам только для чтения. Это предотвратит ошибки, вызываемые несовместимостью чтения-записи. Например, новый накопитель может выбрасывать носители, записанные в формате, который он не поддерживает, сразу после загрузки в накопитель. Или же новый накопитель может не выполнить первую команду записи на носитель, частично записанный в неподдерживаемом формате.

Когда данные на носителе, предназначенном только для чтения, устареют и том будет высвобожден, нужно будет заменить его носителем, полностью совместимым с новым накопителем. Ошибки могут возникать, если новому накопителю не удается правильно откалибровать том, записанный в старом формате. Чтобы избежать этой проблемы, убедитесь, что исходный накопитель находится в исправном рабочем состоянии, а его микрокод - на текущем уровне.

Операции с чистящими картриджами

Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Мониторинг процесса очистки
: Если в библиотеке активируется чистящий картридж и нужно очистить накопитель, сервер размонтирует том данных и запустит операцию очистки. Если операция очистки завершится неудачно или будет отменена либо если чистящего картриджа нет, вы можете не узнать, что требуется очистка накопителя. Из-за этой проблемы необходимо следить за сообщениями об очистке, чтобы обеспечить своевременную очистку накопителей. При необходимости введите команду CLEAN DRIVE, чтобы сервер попытался еще раз произвести очистку, или вручную загрузите чистящий картридж в накопитель.

Использование нескольких чистящих картриджей
: Сервер будет использовать чистящий картридж для числа очисток, указанного при регистрации чистящего картриджа. Если зарегистрировать два или несколько чистящих картриджей, сервер будет использовать только один из них, пока не будет достигнуто заданное для картриджа число очисток. Затем сервер использует следующий чистящий картридж. Если зарегистрировать два или несколько чистящих картриджей и ввести две или несколько команд CLEAN DRIVE одновременно, сервер будет использовать несколько картриджей одновременно и зарегистрирует оставшееся количество очисток для каждого картриджа.

Ссылки, связанные с данной:
AUDIT LIBRARY (аудит томов автоматизированной библиотеки)
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
CLEAN DRIVE (очистка накопителя)
LABEL LIBVOLUME (запись метки на том библиотеки)
Информация, связанная с данной:

QUERY LIBVOLUME (Запросить информацию о томе библиотеки)

Проверка на соответствие лицензии

Убедитесь, что ваше решение IBM Spectrum Protect соответствует положениям вашего лицензионного соглашения. Регулярно производя мониторинг решения, можно отслеживать тенденции роста данных или использование единиц мощности процессора (processor value unit, PVU). Используйте эту информацию, чтобы спланировать будущее приобретение лицензий.

Об этой задаче

Метод, который вы используете, чтобы убедиться, что ваше решение соответствует условиям лицензии, зависит от положений вашего лицензионного соглашения IBM Spectrum Protect.

Фронтальное лицензирование мощности
: Фронтальная модель определяет требования к лицензии на основе объема первичных данных, о которых клиентами было сообщено, что для них создавались резервные копии. К клиентам относятся приложения, виртуальные машины и компьютеры.

Внутреннее лицензирование мощности
: Внутренняя модель определяет требования к лицензии на основе числа терабайт данных, которые хранятся в первичных пулах хранения и репозиториях.
Советы:

- Чтобы обеспечить точность оценки фронтальной и внутренней емкости, установите новейшую версию программы клиента на каждом клиентском узле.
- Информация о фронтальной и внутренней емкости в Центр операций предназначена только для планирования и оценки.

Лицензирование PVU
: Модель PVU основана на использовании PVU серверными устройствами.
Важное замечание: Расчеты PVU, выполняемые IBM Spectrum Protect, считаются оценочными и не имеют юридической силы. Информация о лицензировании PVU, сообщенная продуктом IBM Spectrum Protect, не рассматривается как допустимая замена для IBM® License Metric Tool.

Самую последнюю информацию о моделях лицензирования смотрите в информации о продукте и лицензии на веб-сайте семейства продуктов IBM Spectrum Protect. Если у вас возникнут вопросы или замечания, касающиеся требований по лицензированию, обращайтесь к вашему поставщику программы IBM Spectrum Protect.

Процедура

Чтобы отследить соответствие лицензии, выполните шаги, соответствующие положениям вашего лицензионного соглашения.
Совет: Центр операций обеспечивает электронный отчет, в котором просуммировано использование фронтальной и внутренней емкости. Отчеты можно автоматически регулярно отправлять одному или нескольким получателям. Чтобы сконфигурировать электронные отчеты и управлять ими, щелкните по Отчеты в строке меню Центр операций.

Опция	Описание

Опция	Описание
Фронтальная модель	a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. На странице Фронтальное использование показана оценка фронтальной емкости. b. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости. c. Чтобы оценить емкость для клиентов, которые не сообщают об использовании емкости, перейдите на следующий FTP-сайт, где представлены инструменты измерения и инструкции: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Чтобы изменить фронтальную емкость в соответствии со сценарием, выполните инструкции в самом последнем доступном руководстве по лицензированию. d. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария. e. Убедитесь, что оценка емкости соответствует вашему лицензионному соглашению.
Внутренняя модель	Ограничение: Если исходный и целевой серверы репликации не используют одни и те же параметры политики, вы не сможете использовать Центр операций для мониторинга использования внутренней емкости для реплицируемых клиентов. Информацию о том, как оценить использование емкости для этих клиентов, смотрите в следующей публикации technote 1656476. a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. b. Щелкните по вкладке Внутренний. c. Проверьте, соответствует ли оценка объема данных вашему лицензионному соглашению.
Модель PVU	Иформацию о том, как оценить соответствие условиям лицензирования PVU, смотрите в разделе Оценка соответствия модели лицензирования PVU.

Состояние системы отслеживания с использованием отчетов по электронной почте

Настройте компонент Центр операций, чтобы сгенерировать отчеты по электронной почте, в которых суммируется состояние системы. Вы можете сконфигурировать соединение с почтовым сервером, изменить параметры отчета и (необязательно) создать пользовательские отчеты.

Прежде чем начать

Прежде чем настраивать отчеты по электронной почте, убедитесь, что выполнены следующие требования:

- Доступен хост-сервер Simple Mail Transfer Protocol (SMTP) для отправки и получения отчетов по электронной почте. Сервер SMTP должен быть сконфигурирован как открытый почтовый ретранслятор. Вы также должны убедиться, что у сервера IBM Spectrum Protect, который отправляет сообщения электронной почты, есть доступ к серверу SMTP. Если центр операций установлен на отдельном компьютере, этому компьютеру не требуется доступ к серверу SMTP.
- Чтобы задавать отчеты по электронной почте, нужно иметь системные полномочия для сервера.
- Чтобы задать получателей, можно ввести один или несколько адресов электронной почты или ID администраторов. Если вы собираетесь ввести ID администратора, ID должен быть зарегистрирован на хаб-сервере и с ним должен быть связан адрес электронной почты. Чтобы задать адрес электронной почты для администратора, используйте параметр EMAILADDRESS в команде UPDATE ADMIN.

Об этой задаче

Вы можете сконфигурировать Центр операций для отправки отчета об общих операциях, отчета о соответствии лицензии, а также одного или нескольких пользовательских отчетов. Вы создаете пользовательские отчеты, выбирая шаблоны из набора обычно используемых шаблонов отчетов или вводя операторы SQL SELECT, чтобы запросить информацию на управляемых серверах.

Процедура

Чтобы настроить электронные отчеты и управлять ими, сделайте следующее:

1. В строке меню компонента Центр операций выберите Отчеты.
2. Если соединение с сервером электронной почты еще не сконфигурировано, щелкните по Сконфигурировать почтовый сервер и заполните поля. После того как вы сконфигурируете почтовый сервер, будут включены отчет об общих операциях и отчет о соответствии лицензии.
3. Чтобы изменить параметры отчета, выберите отчет, щелкните по Сведения и обновите форму.
4. Необязательно: Чтобы добавить пользовательский отчет, щелкните по + Отчет и заполните поля.
   Совет: Чтобы сразу же запустить и отправить отчет, выберите отчет и нажмите на Отправить.

Результаты

Разрешенные отчеты будут отправлены в соответствии с заданными параметрами.

Дальнейшие действия

Отчет об общих операциях содержит вложение. Чтобы найти более подробную информацию, разверните разделы во вложении.

Если вам не удается увидеть изображение в отчете, возможно, вы используете клиент электронной почты, который преобразует HTML в другой формат. Информацию об ограничениях смотрите в электронной справке по компоненту Центр операций.

Управление операциями для ленточного решения

Используйте эту информацию для управления операциями для реализации ленточного решения на сервере IBM Spectrum Protect.

- Управление Центром операций
  Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect.
- Управление операциями клиентов
  Вы можете устранить ошибки клиентов, управлять обновлением клиентов и списывать узлы клиентов, которые больше не нужны. Чтобы высвободить пространство хранения на сервере, можно деактивировать устаревшие данные, сохраненные клиентами приложений.
- Управление хранилищем данных
  Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.
- Управление ленточными устройствами
  Стандартные операции с лентами включают подготовку ленточных томов для использования, управления, как и когда тома используются снова, и обеспечение, что доступно достаточно томов. Надо также отвечать на запросы, адресованные оператору, и управлять библиотеками, накопителями, дисками, путями и устройствами перемещения данных.
- Управление ленточными накопителями
  Вы можете запрашивать информацию о ленточных накопителях, обновлять их или удалять. Можно также очищать ленточные устройства и конфигурировать шифрование ленточного устройства и проверку правильности данных.
- Защита сервера IBM Spectrum Protect
  Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.
- Остановка и запуск сервера
  Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.

- Планирование обновления сервера
  Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.
- Подготовка к отключению или обновлению системы
  Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.
- Подготовка к аварии и восстановление после аварии с использованием DRM
  В IBM Spectrum Protect есть функция disaster recovery manager (DRM) для восстановления данных сервера и клиента при аварии.

Управление Центром операций

Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect.

Об этой задаче

Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect. Дополнительную информацию об использовании Центр операций смотрите в разделе Управление Центром операций.

Управление операциями клиентов

Вы можете устранить ошибки клиентов, управлять обновлением клиентов и списывать узлы клиентов, которые больше не нужны. Чтобы высвободить пространство хранения на сервере, можно деактивировать устаревшие данные, сохраненные клиентами приложений.

Об этой задаче

В некоторых случаях ошибки клиентов можно устранить, остановив и перезапустив приемник клиента. Если клиентские узлы или ID администратора окажутся заблокированы, вы сможете устранить проблему, разблокировав клиентский узел или ID администратора, а затем переустановив пароль.

Подробные инструкции по выявлению и устранению ошибок клиентов смотрите в разделе Устранение проблем клиентов.

Инструкции по добавлению клиентов смотрите в разделе Защита приложений и компьютеров.

- Оценка ошибок в журналах ошибок клиентов
  Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.
- Остановка и перезапуск приемника клиента
  Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.
- Изменение паролей
  Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.
- Управление обновлениями клиентов
  Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).
- Списание клиентского узла
  Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).
- Деактивация данных для высвобождения пространства хранения
  В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени,

деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Оценка ошибок в журналах ошибок клиентов

Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.

Прежде чем начать

(Необязательно) Чтобы устранить ошибки на клиенте резервного копирования и архивирования в операционной системе Linux или Windows, убедитесь, что у вас установлен и запущен компонент служба управления клиентами. Инструкции по установке смотрите в разделе Установка службы управления клиентом.

Процедура

Чтобы диагностировать и устранить ошибки клиента, выполните одно из следующих действий:

- Если служба служба управления клиентами установлена на клиентском узле, выполните следующие шаги:
  1. На странице обзора в компоненте Центр операций щелкните по Клиенты и выберите клиент.
  2. Щелкните по Сведения.
  3. На странице Сводка клиента щелкните по вкладке Диагностика.
  4. Прочтите полученные сообщения журнала.
     Советы:
     - Чтобы показать или скрыть панель Журналы клиента, дважды щелкните по строке Журналы клиента.
     - Чтобы изменить размер панели Журналы клиента, щелкните по строке Журналы клиента и перетащите ее в нужное положение.

     Если на странице Диагностика показаны рекомендации, выберите рекомендацию. В панели Журналы клиента сообщения журнала клиента, с которыми связаны рекомендации, выделены.
  5. Используйте рекомендации, чтобы устранить проблемы, указанные в сообщениях об ошибках.
     Совет: Рекомендации предоставляются не для всех сообщений клиентов.
- Если служба служба управления клиентами не установлена на клиентском узле, смотрите журналы ошибок установленного клиента.

Остановка и перезапуск приемника клиента

Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

Об этой задаче

В некоторых случаях ошибки планирования клиентов можно устранить, остановив и перезапустив приемник клиента. Чтобы запланированные операции могли выполняться на клиенте, приемник клиента должен работать. Например, если вы измените IP-адрес или имя домене сервера, вы должны будете перезапустить приемник клиента.

Процедура

Следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- Чтобы остановить приемник клиента, выполните следующие действия:
  a. Определите ID процесса приемника клиента, введя в командной строке следующую команду:

     ```
     ps -ef | grep dsmcad
     ```

     Ознакомьтесь с выводом. В приведенном ниже примере выходной информации 6764 - это ID процесса приемника клиента:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

b. Введите следующую команду в командной строке:

```
kill -9 PID
```

где *PID* задает ID процесса приемника клиента.

- Чтобы запустить приемник клиента, введите в командной строке следующую команду:

```
/usr/bin/dsmcad
```

Linux

- Чтобы остановить приемник клиента (но не перезапускать его), введите следующую команду:

```
# service dsmcad stop
```

- Чтобы остановить и перезапустить приемник клиента, введите следующие команды:

```
# service dsmcad restart
```

MAC OS X

Выберите Приложения > Утилиты > Терминал.

- Чтобы остановить приемник клиента, введите следующую команду:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Чтобы запустить приемник клиента, введите следующую команду:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Чтобы остановить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Остановить и OK.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Запуск и OK.

Ссылки, связанные с данной:
Устранение проблем расписаний клиентов

Изменение паролей

Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

Процедура

Чтобы устранить ошибки паролей, выполните одно из следующих действий:

- Если клиент резервного копирования и архивирования установлен на клиентском узле, а пароль был потерян или забыт, выполните следующие шаги:
  1. Сгенерируйте новый пароль, введя команду UPDATE NODE:

     ```
     update node имя_узла
     новый_пароль forcepwreset=yes
     ```

     где *имя_узла* - это клиентский узел, а *новый_пароль* - это пароль, который вы назначаете.
  2. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.

Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

- Если администратор окажется заблокирован из-за проблем, связанных с паролем, выполните следующие шаги:
  1. Чтобы обеспечить администратору доступ к серверу, введите команду UNLOCK ADMIN. Инструкции смотрите в разделе UNLOCK ADMIN (разблокирование администратора).
  2. Задайте новый пароль, используя команду UPDATE ADMIN:

     ```
     update admin имя_администратора
     новый_пароль
     forcepwreset=yes
     ```

     где *имя_администратора* - это имя администратора, а *новый_пароль* - это пароль, который вы назначаете.
- Если клиентский узел заблокирован, выполните следующие шаги:
  1. Определите, почему клиентский узел заблокирован и нужно ли его разблокировать. Например, если клиентский узел окажется списан, он удаляется из производственной среды. Обратить операцию списания нельзя, и клиентский узел останется заблокированным. Клиентский узел также может оказаться заблокированным, если данные клиента являются предметом юридического изучения.
  2. Если вам нужно разблокировать клиентский узел, используйте команду UNLOCK NODE. Инструкции смотрите в разделе UNLOCK NODE (Разблокировать клиентский узел).
  3. Сгенерируйте новый пароль, введя команду UPDATE NODE:

     ```
     update node имя_узла
     новый_пароль forcepwreset=yes
     ```

     где *имя_узла* задает имя узла, а *новый_пароль* - это пароль, который вы назначаете.
  4. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
     Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

Управление обновлениями клиентов

Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Прежде чем начать

1. Прочтите требования к совместимости клиентов/серверов в разделе Техническое замечание 1053218. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены.
2. Узнайте о требованиях к системе для клиента в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
3. Если решение содержит агенты хранения или библиотечные клиенты, ознакомьтесь с информацией о совместимости агентов хранения и библиотечных клиентов с серверами, сконфигурированными в качестве менеджеров библиотек. Смотрите раздел Техническое замечание 1302789.

   Если вы собираетесь обновить менеджера библиотек и библиотечный клиент, сначала нужно обновить менеджера библиотек.

Процедура

Для обновления программного обеспечения выполните инструкции, перечисленные в следующей таблице.

Программа	**Ссылка на инструкции**
Клиент резервного копирования и архивирования IBM Spectrum Protect	• Планирование обновлений клиента

Программа	Ссылка на инструкции
IBM Spectrum Protect Snapshot	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Databases	• Обновление Data Protection for SQL Server • Установка Data Protection for Oracle • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0) • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Установка и обновление Data Protection for VMware • Установка Data Protection for Microsoft Hyper-V

Списание клиентского узла

Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).

Об этой задаче

При запуске процесса списания сервер блокирует клиентский узел, чтобы помешать ему получить доступ к серверу. Файлы, принадлежащие клиентскому узлу, постепенно удаляются, и затем удаляется клиентский узел. Можно списать следующие типы клиентских узлов:

Клиентские узлы приложения
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Клиентские узлы компьютеров
: В число клиентских узлов компьютеров входят рабочие станции, серверы файлов NAS и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Простейший метод списания клиентского узла заключается в том, чтобы использовать Центр операций. Процесс списания выполняется в фоновом режиме. Если клиент сконфигурирован для репликации данных клиента, Центр операций, прежде чем списать клиент, автоматически удалит клиент из репликации на исходном и целевом серверах репликации.

Совет: Либо можно списать клиентский узел, введя команду DECOMMISSION NODE или DECOMMISSION VM. Вы можете счесть целесообразным использовать этот метод в следующих случаях:

- Чтобы запланировать процесс списания на будущее или выполнить ряд команд, используя сценарий, задайте выполнение процесса списания в фоновом режиме.
- Чтобы производить мониторинг процесса списания с целью отладки, задайте выполнение процесса списания в фоновом режиме. Если вы запустите процесс в активном режиме, вам придется дождаться завершения процесса, прежде чем вы сможете перейти к другим задачам.

Процедура

Выполните одно из следующих действий.

- Чтобы списать клиент в фоновом режиме, используя Центр операций, выполните следующие действия:
  1. На странице Обзор для компонента Центр операций щелкните по Клиенты и выберите клиент.
  2. Выберите Еще > Списать.
- Чтобы списать клиентский узел, используя команду администрирования, выполните одно из следующих действий:
  - Чтобы списать клиентские узлы приложений или системные клиентские узлы в фоновом режиме, введите команду DECOMMISSION NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

    ```
    decommission node austin
    ```

  - Чтобы списать клиентские узлы приложений или системные клиентские узлы в активном режиме, введите команду DECOMMISSION NODE и задайте параметр `wait=yes`. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

    ```
    decommission node austin wait=yes
    ```

  - Чтобы списать виртуальную машину в фоновом режиме, введите команду DECOMMISSION VM. Например, если имя виртуальной машины - AUSTIN, файловое пространство - 7, а имя файлового пространства задано с помощью ID файлового пространства, введите следующую команду:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

    ```
    decommission vm "austin 2" 7 nametype=fsid
    ```

  - Чтобы списать виртуальную машину в активном режиме, введите команду DECOMMISSION VM и задайте параметр `wait=yes`. Например, введите следующую команду:

    ```
    decommission vm austin 7 nametype=fsid wait=yes
    ```

    Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

    ```
    decommission vm "austin 2" 7 nametype=fsid wait=yes
    ```

Дальнейшие действия

Следите за сообщениями об ошибках, которые могут появиться в пользовательском интерфейсе или в выходной информации команды сразу после запуска процесса.

Можно проверить, списан ли клиентский узел:

1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты.
2. В таблице Клиенты проверьте состояние в столбце Под угрозой:
   - Состояние DECOMMISSIONED (Списан) указывает, что узел списан.
   - Нулевое значение указывает, что узел не списан.
   - Состояние PENDING (Отложено) указывает, что узел списывается или процесс списания завершился неудачно.

   Совет: Если вы хотите определить состояние отложенного процесса списания, введите следующую команду:

   ```
   query process
   ```

3. Ознакомьтесь с выводом команды:
   - Если указано состояние для процесса списания, процесс выполняется. Например:

     ```
     query process

      Номер       Описание процесса                  Состояние процесса
       Число
     --------     --------------------     -----------------------------------------
            3          DECOMMISSION NODE        Number of backup objects deactivated
                                                for node NODE1: 8 objects deactivated.
     ```

   - Если для процесса списания никакого состояния не указано и вы не получили сообщения об ошибке, процесс не завершен. Процесс может быть не завершен, если файлы, связанные с узлом, еще не деактивированы. После деактивации файлов снова запустите процесс списания.
   - Если для процесса списания никакого состояния не указано и вы получили сообщения об ошибке, это означает, что процесс завершился неудачно. Еще раз запустите процесс списания.

Ссылки, связанные с данной:
DECOMMISSION NODE (Списать клиентский узел)
DECOMMISSION VM (Списать виртуальную машину)

Деактивация данных для высвобождения пространства хранения

В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Об этой задаче

Некоторые клиенты приложений всегда сохраняют данные на сервере как активные резервные копии данных. Поскольку активные резервные копии данных не управляются политиками устаревания перечня, данные не удаляются автоматически, и серверное хранилище используется до бесконечности. Чтобы высвободить пространство хранения, используемое устаревшими данными, можно деактивировать данные.

Когда вы запускаете процесс деактивации, все активные резервные копии данных, сохраненные до указанной даты, станут неактивными. Данные будут удалены по мере истечения срока их хранения, и восстановить их будет нельзя. Функция деактивации применяется только к клиентам приложений, которые защищают базы данных Oracle.

Процедура

1. На странице обзора в компоненте Центр операций щелкните по Клиенты.
2. В таблице Клиенты выберите один или несколько клиентов и щелкните по Еще > Очистить.
   Метод командной строки: Деактивируйте данные, используя команду DEACTIVATE DATA.

Ссылки, связанные с данной:
DEACTIVATE DATA (деактивация данных для клиентского узла)

Управление хранилищем данных

Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.

- Управление емкостью перечня
  Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.
- Тонкая настройка запланированных операций
  Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.
- Оптимизация операций путем включения совместного размещения файлов клиентов
  Совместное размещение файлов клиентов сокращает число монтирований томов, которые требуются, когда

пользователи восстанавливают, получают или возвращают много файлов из пула хранения. В результате сокращается общее время выполнения этих операций.

Ссылки, связанные с данной:
Типы пулов хранения

Управление емкостью перечня

Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

Прежде чем начать

У активного и архивного журналов есть следующие особенности:

- Максимальный размер активного журнала равен 512 ГБ. Более подробную информацию о размерах активного журнала для вашей системы смотрите в разделе Планирование массивов хранения.
- Размер архивного журнала ограничен размером файловой системы, в которой он установлен. Размер архивного журнала не поддерживается на заранее заданном уровне, как в случае активного журнала. Архивные файлы журналов автоматически удаляются, когда они становятся больше не нужны.

(Необязательно) Лучше всего создать архивный журнал отказоустойчивости, чтобы сохранять файлы архивного журнала при переполнении каталога архивных журналов.

Проверьте Центр операций, чтобы определить, какой компонент перечня переполняется. Прежде чем увеличивать размер одного из компонентов перечня, убедитесь, чтобы вы остановили сервер.

Процедура

- Чтобы увеличить размер дискового пространства для базы данных, выполните следующие шаги:
  - Создайте один или несколько каталогов для базы данных на отдельных накопителях или в файловых системах.
  - Введите команду EXTEND DBSPACE, чтобы добавить каталог или каталоги к базе данных. Каталоги должны быть доступны для ID пользователя экземпляра менеджера базы данных. По умолчанию данные перераспределяются по всем каталогам базы данных и пространство высвобождается.
    Советы:
    - Время, необходимое для полного перераспределения данных и высвобождения пространства, изменяется в зависимости от размера вашей базы данных. Убедитесь, что это учтено при планировании.
    - Убедитесь, что размер указанных каталогов совпадает с размером существующих каталогов, чтобы обеспечить согласованную степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.
  - Остановите и перезапустите сервер для полного использования новых каталогов.
  - Если потребуется, исправьте базу данных. Реорганизация индекса и таблиц для базы данных сервера может помочь избежать неожиданных проблем, связанных с ростом базы данных и производительностью. Дополнительную информацию о реорганизации базы данных смотрите в Техническое замечание 1683633.
- Чтобы узнать, как уменьшить размер базы данных для серверов V7.1 и новее, смотрите информацию в разделе Техническое замечание 1683633.
  Ограничение: Команды могут увеличить число операций ввода-вывода и повлиять на производительность сервера. Чтобы свести к минимуму проблемы производительности, подождите выполнения одной команды перед вводом следующей команды. Команды DB2 можно вводить, когда сервер работает.
- Чтобы увеличить или уменьшить размер активного журнала, выполните следующие шаги:
  1. Убедитесь, что в каталоге активного журнала достаточно пространства для увеличения размера журнала.
  2. Отключите сервер.
  3. Измените в файле dsmserv.opt значение опции ACTIVELOGSIZE, задав новый размер активного журнала (в мегабайтах).
     Размер файла активного журнала основан на значении опции ACTIVELOGSIZE. Рекомендации по требованиям к объему пространства приведены в следующей таблице:

Табл. 1. Как оценить требования к пространству томов и файлов

Значение опции ACTIVELOGSize	Зарезервируйте этот объем свободного пространства в каталоге активного журнала в дополнение к пространству ACTIVELOGSize.
16 ГБ - 128 ГБ	5120 МБ
129 ГБ - 256 ГБ	10240 МБ
257 ГБ - 512 ГБ	20480 МБ

Чтобы изменить размер активного журнала до максимального размера, равного 512 ГБ, введите следующую серверную опцию:

```
activelogsize 524288
```

4. Если вы собираетесь использовать новый каталог активного журнала, измените имя каталога, заданное серверной опцией ACTIVELOGDIRECTORY. Новый каталог должен быть пустым, и он должен быть доступен для ID пользователя менеджера базы данных.
5. Перезапустите сервер.

- Произведите сжатие архивных журналов, чтобы уменьшить объем пространства, необходимого для хранения. Разрешите динамическое сжатие архивного журнала следующей командой:

  ```
  setopt archlogcompress yes
  ```

  Ограничение: Будьте внимательны, если вы разрешаете опцию сервера ARCHLOGCOMPRESS на компьютерах с постоянным высоким использованием томов и высокими рабочими нагрузками. Разрешение этой опции в такой среде может привести к задержкам при архивировании файлов журнала из файловой системы активного журнала в файловую систему архивного журнала. Задержка может привести к тому, что в файловой системе активного журнала не хватит места. Обязательно выполняйте мониторинг пространства, доступного в файловой системе активного журнала, после разрешения сжатия архивного журнала. Если использование файловой системы каталога активного журнала приближается к предельному, то запретите опцию сервера ARCHLOGCOMPRESS. Чтобы немедленно запретить сжатие архивного журнала без остановки сервера, введите команду SETOPT.

Ссылки, связанные с данной:
ACTIVELOGSIZE, серверная опция
EXTEND DBSPACE (увеличение емкости базы данных)
SETOPT (Задать динамическое обновление серверной опции)

Тонкая настройка запланированных операций

Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Процедура

1. Регулярно отслеживайте производительность системы, чтобы убедиться, что задачи по резервному копированию и обслуживанию выполняются успешно. Дополнительную информацию о мониторинге смотрите в разделе Мониторинг ленточного решения.
2. Если информация мониторинга показывает, что рабочая нагрузка сервера повышается, вам, возможно, следует проверить информацию планирования. Проверьте, является ли емкость системы достаточной, в следующих случаях:
   - Число клиентов увеличивается
   - Объем данных, резервное копирование которых производится, возрастает
   - Время, доступное для резервного копирования, изменяется
3. Определите, есть ли в вашем решении проблемы, отрицательно влияющие на производительность. Проверьте расписания клиентов, чтобы выяснить, выполняются ли задачи в течение запланированного периода времени:
   a. Выберите клиента на странице Клиенты Центра операций.
   b. Щелкните по Сведения.
   c. На странице Сводка на клиенте проверьте операции Создана резервная копия и Реплицирован, чтобы выявить все риски.

   Скорректируйте время и частоту операций резервного копирования клиента, если потребуется.
4. Запланируйте достаточно времени для следующих задач по обслуживанию, чтобы они успешно выполнялись в течение 24-часового периода:
   a. Создание резервной копии базы данных

b. Запускайте обработку устаревания, чтобы удалить резервные и архивные копии файлов из серверного хранилища.

Понятия, связанные с данным:
Производительность
Задачи, связанные с данной:
Дедупликация данных (V7.1.1)

Оптимизация операций путем включения совместного размещения файлов клиентов

Совместное размещение файлов клиентов сокращает число монтирований томов, которые требуются, когда пользователи восстанавливают, получают или возвращают много файлов из пула хранения. В результате сокращается общее время выполнения этих операций.

Об этой задаче

При включенном совместном размещении сервер пытается разместить все файлы в минимальном количестве томов хранения с последовательным доступом. Эти файлы могут принадлежать к одному клиентскому узлу, к группе клиентских узлов, к файловому пространству или к группе файловых пространств. Совместное размещение можно задать для каждого пула устройств с последовательным доступом при создании определения этого пула или при обновлении его характеристик.

Рис. 1 демонстрирует пример совместного размещения данных на уровне клиентского узла для трех клиентов — данные каждого из них содержатся на отдельном томе.

Рис. 1. Пример совместного размещения, разрешаемого на узле

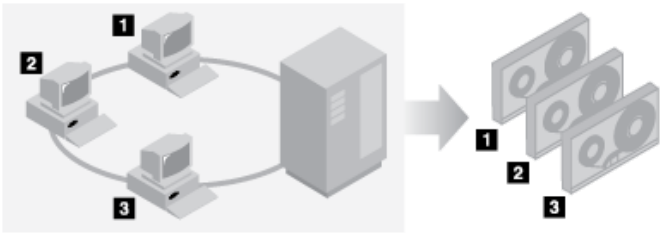


Рис. 2 демонстрирует пример совместного размещения данных на уровне группы клиентских узлов. Всего определены три группы, и данные каждой из них хранятся на отдельном наборе томов.

Рис. 2. Пример совместного размещения, разрешаемого в группе совместного размещения на узле

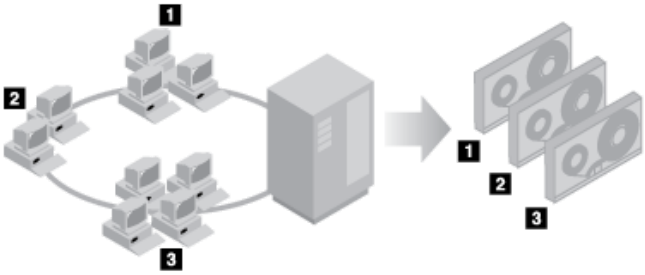
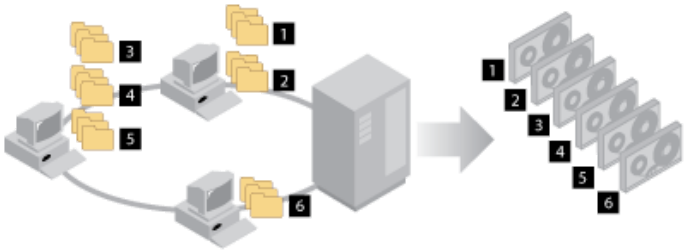


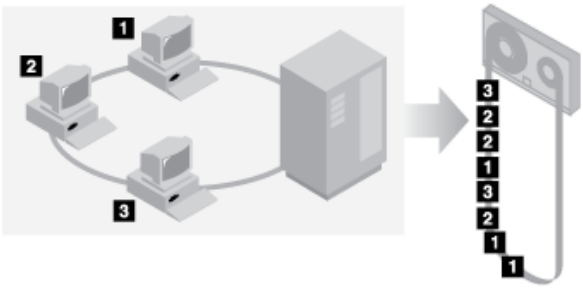
Рис. 3 демонстрирует пример совместного размещения данных на уровне групп из файловых пространств. Определено шесть групп. Каждая группа содержит данные из файловых пространств, принадлежащих одному узлу. Данные для каждой группы хранятся в отдельном томе.

Рис. 3. Пример совместного размещения, разрешенного в группе совместного размещения файлового пространства



Когда функция совместного размещения отключена, сервер пытается использовать все доступное пространство очередного тома назначения, и только потом начинает запись на следующий том. Хотя такой способ работы позволяет обходиться меньшим числом томов, пользовательские файлы оказываются разбросанными по многим томам. Рис. 4 демонстрирует пример конфигурации с отключенной функцией совместного размещения, когда пространство одного тома совместно используется тремя клиентами.

Рис. 4. Пример конфигурации с отключенной функцией совместного размещения



Когда функция совместного размещения отключена, при выполнении пользовательских операций восстановления, извлечения из архива или возврата большого количества файлов производится большее число операций монтирования томов.

По умолчанию для первичных пулов томов с последовательным доступом сервер IBM Spectrum Protect осуществляет совместное размещение на уровне группы. Для пулов хранения копий функция совместного размещения по умолчанию отключена.

- Влияние функции совместного размещения на выполнение операций
  Влияние функции совместного размещения на ресурсы и производительность системы зависит от типа выполняемых операций.
- Выбор томов с включенным совместным размещением
  Выбор томов зависит от того, производится ли совместное размещение по группам, узлам или файловым пространствам.
- Выбор томов с выключенным совместным размещением
  Когда функция совместного размещения отключена, сервер сначала пытается использовать все свободное пространство одного тома и лишь потом обращается к следующему тому.
- Параметры совместного размещения
  Существует возможность изменить параметр совместного размещения для уже заданного пула хранения, обновив характеристики этого пула хранения. Это изменение не повлияет на размещение файлов, уже находящихся в пуле.
- Совместное размещение пулов хранения копий
  Применение функции совместного размещения для пулов хранения копий должно осуществляться с особой осторожностью. Совместное размещение пулов хранения копий, особенно на узле или в файловом пространстве, приводит к увеличению числа частично заполненных томов, а также к выполнению потенциально ненужных операций высвобождения пространства.
- Планирование применения и активизация функции совместного размещения
  Имея представление о результатах применения совместного размещение, можно сократить число операций монтирования носителей, более рационально использовать пространство на томах с последовательным доступом и повысить эффективность операций сервера.

Влияние функции совместного размещения на выполнение операций

Влияние функции совместного размещения на ресурсы и производительность системы зависит от типа выполняемых операций.

Табл. 1 содержит сводную информацию о воздействии функции совместного размещения на выполнение различных операций.

Табл. 1. Влияние функции совместного размещения на выполнение операций

Операция	**Функция совместного размещения включена**	**Функция совместного размещения отключена**
Резервное копирование, архивация или перенос клиентских файлов	Для совместного размещения файлов производится больше операций монтирования	Требуется меньше операций монтирования носителей.
Восстановление, извлечение или возврат клиентских файлов	Восстановление, извлечение из архива или возврат большого количества клиентских файлов производится быстрее, поскольку файлы размещены на меньшем числе томов	Для каждого пользователя может производиться несколько операций монтирования, поскольку файлы бывают разбросаны по разным томам. На одном томе с последовательным доступом могут находиться файлы нескольких пользователей. Например, если два пользователя пытаются восстановить файлы в одном томе, один из пользователей будет вынужден дожидаться, когда будут восстановлены файлы другого пользователя.
Сохранение данных на ленте	Сервер задействует большое число ленточных томов, пытаясь сохранять файлы разных пользователей на разных томах, и лишь когда доступного пространства не остается, он может записать файлы разных пользователей на один том.	Сервер пытается использовать все доступное пространство очередной ленты, и лишь когда оно исчерпывается, сервер начинает использовать другую ленту.
Монтирование носителей	При резервном копировании, архивировании или переносе клиентских файлов прямо на тома с последовательным доступом требуется большее число операций монтирования. Также больше операций монтирования требуется при консолидации остаточных данных и при переносе данных из пула хранения. Управляется большее число томов, поскольку они заполняются не до конца.	При восстановлении, извлечении из архива и возврате клиентских файлов требуется больше операций монтирования.
Генерирование резервных наборов	Тратится меньше времени на поиск записей в базах данных и требуется выполнение меньшего количества операций монтирования.	Тратится больше времени на поиск записей в базах данных и требуется выполнение меньшего количества операций монтирования.

Если для группы, одного узла клиента или файлового пространства включено совместное размещение, все данные, принадлежащие этой группе, узлу или файловому пространству, перемещаются или копируются в ходе одного серверного

процесса. Например, если данные совместно размещаются по группам, все данные для всех узлов, принадлежащих одной группе совместного размещения, переносятся одним процессом.

При совместном размещении данных сервер IBM Spectrum Protect пытается разместить все файлы на минимальном числе томов с последовательным доступом. Однако, когда сервер выполняет резервное копирование данных на тома с последовательным доступом, установки резервного копирования имеют приоритет перед установками совместного размещения. В результате этого сервер выполняет операцию резервного копирования, но не может совместное разместить данные.

Предположим, например, что совместное размещение осуществляется на уровне узла и этому узлу разрешено использовать две точки монтирования на сервере. Предположим также, что данные, резервно копируемые с этого узла, легко помещаются на один ленточный том. Выполняя резервное копирование, сервер может смонтировать два тома, и в результате данные узла могут оказаться распределенными между двумя лентами. Если включить совместное размещение, следующие операции сервера будут использовать один серверный процесс:

- Перемещение данных с томов с произвольным или последовательным доступом.
- Перемещение данных узла с томов с последовательным доступом.
- Резервное копирование пула хранения с произвольным или последовательным доступом.
- Восстановление пула хранения с последовательным доступом.
- Высвобождение пространства в пуле хранения с последовательным доступом или на внесайтовых томах
- Перенос данных из пула хранения с произвольным доступом

При переносе данных из дискового пула хранения с произвольным доступом в пул хранения с последовательным доступом, когда совместное размещение производится на основе узлов или файловых пространств, узлы или файловые пространства автоматически выбираются для переноса на основе объема данных, подлежащего переносу. Для узла или файлового пространства с максимальным количеством таких данных перенос осуществляется в первую очередь. Если же совместное размещение осуществляется на уровне групп узлов, все узлы, связанные с пулом хранения, оцениваются на предмет наличия максимального количества подлежащих переносу данных. Сначала переносятся данные с узла с наибольшим количеством данных вместе со всеми данными для узлов, принадлежащих данной группе совместного размещения. Этот процесс выполняется независимо от того, сколько данных хранится в файловых пространствах узлов, и от того, был ли достигнут нижний порог переноса.

Однако, когда вы переносите совместно размещенные данные из пула хранения с последовательным доступом в другой пул хранения с последовательным доступом, сервер заказывает тома в соответствии с датой, когда в последний раз осуществлялся доступ к тому. Первым переносится том с самой ранней датой обращения к нему, а последним - том с самой поздней датой доступа.

Одной из причин, почему совместное размещение лучше осуществлять по группам, является то, что отдельные клиентские узлы часто не имеют достаточного количества данных для заполнения ленточного тома высокой емкости. Поэтому совместное размещение на уровне групп позволяет уменьшить объем неиспользуемого пространства на лентах. Кроме того, совместное размещение данных по группам файловых пространств значительно сокращает объем неиспользуемых лент.

Данные, принадлежащие ко всем узлам в одной группе совместного размещения, переносятся в одном процессе. Поэтому совместное размещение по группам может сократить число раз, когда нужно монтировать том, подлежащий переносу. А еще при этом ускоряется сканирование базы данных и сокращается число проходов по лентам во время переноса данных из одного пула хранения с последовательным доступом в другой.

Выбор томов с включенным совместным размещением

Выбор томов зависит от того, производится ли совместное размещение по группам, узлам или файловым пространствам.

Табл. 1содержит критерии выбора сервером IBM Spectrum Protect первого тома, когда для пула хранения включена функция совместного размещения на уровне клиентских узлов, их групп или файловых пространств. Эти критерии применяются по очереди в указанном в таблице порядке, то есть в случае, когда отсутствует том, удовлетворяющий критерию 1, сервер ищет том, удовлетворяющий критерию 2 и т. д.

Табл. 1. Как сервер выбирает тома при включенной функции совместного размещения

Критерий выбора тома	Совместное размещение на уровне групп	Совместное размещение на уровне узлов	Совместное размещение на уровне файловых пространств

Критерий выбора тома	Совместное размещение на уровне групп	Совместное размещение на уровне узлов	Совместное размещение на уровне файловых пространств
1	Том, уже содержащий файлы узлов из группы совместного размещения, к которой принадлежит клиент	Том, который уже содержит файлы того же клиентского узла	Том, который уже содержит файлы того же файлового пространства того же клиентского узла
2	Пустой заранее определенный том	Пустой заранее определенный том	Пустой заранее определенный том
3	Пустой чистый том	Пустой чистый том	Пустой чистый том
4	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные	Том, содержащий данные с одного клиентского узла
5	Неприменимо	Неприменимо	Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные

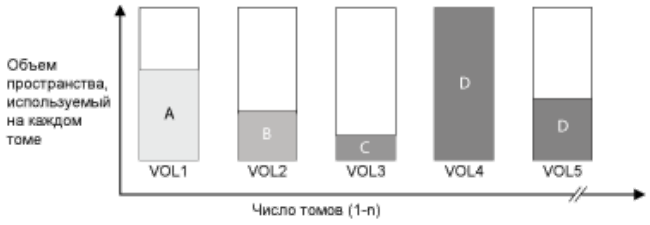
Когда сервер должен продолжить сохранение данных уже во втором томе, он использует следующий порядок выбора для доступности большего пространства:

1. Пустой заранее определенный том
2. Пустой чистый том
3. Том с наибольшим объемом свободного пространства из числа томов, уже содержащих данные
4. Любой доступный том пула хранения

Когда совместное размещение организовано на уровне клиентского узла или файлового пространства, сервер пытается обеспечить наилучшее использование индивидуальных томов и минимизировать в томах перемешивание файлов от различных клиентов или из разных файловых пространств. Эта конфигурация показана на Рис. 1, где видно, что выбор томов осуществляется *по горизонтали*, то есть перед тем, как будет использовано все доступное пространство каждого тома, осуществляется запись на все доступные тома. A, B, C и D - это файлы с четырех разных клиентских узлов.
Советы:

1. Если совместное размещение осуществляется на уровне клиентских узлов и узел содержит несколько файловых пространств, сервер не пытается совместно размещать файлы каждого из файловых пространств.
2. Если совместное размещение осуществляется на уровне файловых пространств и узел содержит их несколько, сервер пытается размещать файлы разных файловых пространств на разных томах.

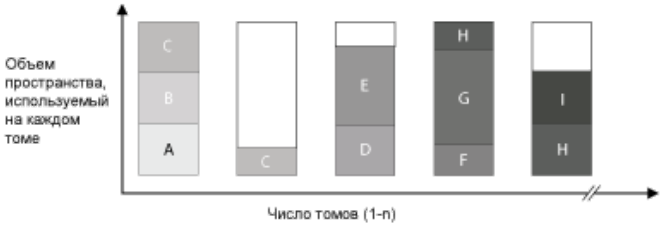
Рис. 1. Использование всех доступных томов хранения с последовательным доступом с включенным совместным размещением на уровне узлов или файловых пространств



Совместное размещение может производиться на основе группы файловых пространств или группы узлов. Когда совместное размещение выполняется по группе узлов (группа совместного размещения по узлам), сервер пытается совместно разместить данные из узлов, принадлежащих к одной группе совместного размещения. Группа совместного размещения на основе файловых пространств использует те же методы, что и группа совместного размещения на основе узлов, но может использовать больше пространства, благодаря детализации размеров файловых пространств. В Рис. 2 показан пример, как размещаются данные для следующих групп узлов:

- группы 1, состоящей из узлов A, B и C;
- группы 2, состоящей из узлов D и E;
- группы 3, состоящей из узлов F, G, H и I

При возможности сервер IBM Spectrum Protect совместно размещает данные, принадлежащие группе узлов на одной ленте, представленной на рисунке Группой 2. Данные одного узла можно распределить также по нескольким лентам, связанным с группой (Группа 1 и Группа 2). Если узлы из одной группы размещения содержат по несколько файловых пространств, сервер не пытается размещать совместно данные каждого конкретного файлового пространства.
Рис. 2. Использование всех доступных томов хранения с последовательным доступом с включенным совместным размещением на уровне групп



Обычно для выполняемой операции сервер IBM Spectrum Protect всегда записывает данные в текущий заполняемый том. Однако иногда можно заметить в совместно размещенном пуле хранения более одного заполняемого тома. В пуле совместного хранения может оказаться несколько заполняемых томов, если различные процессы сервера или сеансы клиента пытаются одновременно сохранить данные в пуле совместного размещения. В этой ситуации IBM Spectrum Protect выделит том для каждого процесса или сеанса, которому требуется том, так чтобы обе операции выполнялись как можно быстрее.

Выбор томов с выключенным совместным размещением

Когда функция совместного размещения отключена, сервер сначала пытается использовать все свободное пространство одного тома и лишь потом обращается к следующему тому.

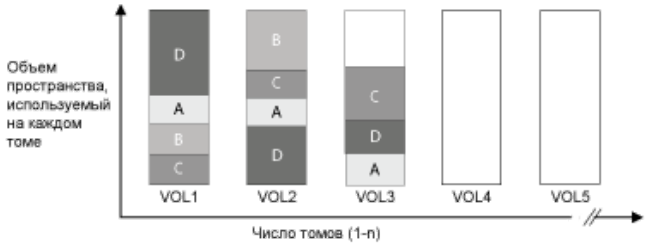
При хранении файлов клиента в пуле хранения с последовательным доступом, для которого выключено совместное размещение, сервер выбирает том, используя следующий порядок выбора:

1. Использовавшийся ранее том с последовательным доступом, на котором имеется свободное пространство (при этом первым выбирается том с наибольшим количеством данных)
2. Пустой том

Когда свободное пространство текущего тома исчерпывается и серверу требуется продолжить сохранение данных на другом томе, он ищет в пуле свободный том. Если никаких пустых томов не существует, сервер попытается выбрать любой из оставшихся доступных томов в пуле хранения.

На Рис. 1 показано, что при выключенном совместном размещении использование томов осуществляется по вертикали. В этом примере используется меньшее число томов, поскольку сервер пытается заполнить все доступное пространство каждого тома, записывая туда файлы разных клиентов. Столбцы A, B, C и D представляют данные с четырех разных клиентских узлов.

Рис. 1. Использование всего доступного пространства на томах с последовательным доступом с выключенным совместным размещением



Параметры совместного размещения

Существует возможность изменить параметр совместного размещения для уже заданного пула хранения, обновив характеристики этого пула хранения. Это изменение не повлияет на размещение файлов, уже находящихся в пуле.

Например, если совместное размещение выключено для пула хранения, а вы его включите, с этого момента файлы клиента, хранящиеся в пуле, будет размещаться совместно. Файлы, которые ранее хранились в пуле хранения, не перемещаются для их совместного размещения. По мере высвобождения томов данные в пуле становятся все менее и менее совместно размещенными. Также можно использовать команды MOVE DATA или MOVE NODEDATA для перемещения данных на новые тома, чтобы повысить степень совместного размещения. Перемещение данных на новые тома вызывает увеличение времени обработки и объема операций монтирования томов.
Совет: Можно столкнуться с ожиданием монтирования, или оно может занимать больше времени, чем обычно, когда включено совместное размещение по файловым пространствам и на узле есть том, содержащий несколько файловых пространств. Если том подлежит приему данных, IBM Spectrum Protect будет ждать этого тома.

Совместное размещение пулов хранения копий

Применение функции совместного размещения для пулов хранения копий должно осуществляться с особой осторожностью. Совместное размещение пулов хранения копий, особенно на узле или в файловом пространстве, приводит к увеличению числа частично заполненных томов, а также к выполнению потенциально ненужных операций высвобождения пространства.

Первичные пулы хранения выполняют роль в восстановлении, отличающуюся от пулов хранения копий. Обычно вы используете первичные пулы хранения для восстановления данных непосредственно на клиентах. В случае серьезной аварии, когда выходят из строя и клиенты, и сервер, можно использовать внесайтовые тома пулов хранения копий для восстановления первичных пулов хранения. Типы сценариев восстановления могут помочь определить, использовать ли совместное размещение в пулах хранения копий.

Обычно большое количество частично заполненных томов появляется при совместном размещении на уровне узлов или файловых пространств. Однако при совместном размещении на уровне групп этот эффект проявляется незначительно. Наличие частично заполненных томов приемлемо для первичных пулов хранения, поскольку такие тома остаются доступными и могут заполняться новыми данными в ходе следующих процессов переноса. Однако частично заполненные тома могут быть неприемлемы для пулов хранения копий, тома пулов хранения которых сразу переводятся в автономный режим. Если вы решите применять совместное размещение для пулов хранения копий, вы окажетесь перед следующим выбором:

- Хранить большее количество частично заполненных томов автономно, увеличивая тем самым частоту операций высвобождения пространства, когда снижается или достигается порог высвобождения томов.
- Оставлять частично заполненные тома подключенными до тех пор, пока они не заполнятся, рискуя утратить их в случае серьезной аварии и в результате не иметь возможности восстановить содержащиеся на них данные;
- Или осуществлять совместное размещение на уровне групп, чтобы использовать максимально возможную емкость ленточных устройств.

Если совместное размещение выключено для пула хранения копий, после резервного копирования данных в пул хранения копий, в нем как правило, остается всего несколько частично заполненных томов.

Внимательно изучите доступные опции перед использованием совместного размещения для пулов хранения, а также для принятия решения об использовании синхронной записи. Если синхронная запись не используется и вы используете совместное размещение для первичных пулов хранения, может потребоваться отключить совместное размещение для пулов хранения копий. Совместное размещение для пулов хранения копий может быть желательно при наличии нескольких клиентов, у каждого из которых каждый день возникает много данных инкрементного резервного копирования. Для совместного размещения с синхронной записью необходимо обеспечить, чтобы параметры совместного размещения были идентичны для первичных пулов хранения и пулов хранения копий.

Планирование применения и активизация функции совместного размещения

Имея представление о результатах применения совместного размещение, можно сократить число операций монтирования носителей, более рационально использовать пространство на томах с последовательным доступом и повысить эффективность операций сервера.

Об этой задаче

Табл. 1 содержит список четырех опций совместного размещения, которые можно задавать в командах DEFINE STGPOOL и UPDATE STGPOOL. В таблице указано также, как совместное размещение влияет на данные из узлов, принадлежащих и не принадлежащих группам совместного размещения.

Табл. 1. Опции совместного размещения и их воздействие на данные узлов

Опция совместного размещения	Узел не является членом ни одной группы совместного размещения	Узел является членом одной из групп совместного размещения
Нет	Для данных этого узла совместное размещение не применяется.	Для данных этого узла совместное размещение не применяется.
Группа	Сервер размещает данные узла на как можно меньшем числе томов в пуле хранения.	Сервер размещает данные узла и других узлов из той же группы совместного размещения на как можно меньшем числе томов
Узел	Сервер размещает данные узла на как можно меньшем числе томов.	Сервер размещает данные узла на как можно меньшем числе томов.
File space	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах

Табл. 2. Опции групп совместного размещения и влияние на данные файлового пространства

Опция совместного размещения	Если файловое пространство не определено как участник группы совместного размещения	Если файловое пространство определено как участник группы совместного размещения
Нет	Данные для файлового пространства совместно не размещаются.	Данные для файлового пространства совместно не размещаются.
Группа	Сервер размещает данные файлового пространства на как можно меньшем числе томов в пуле хранения.	Сервер сохраняет данные для файлового пространства и других файловых пространств, принадлежащих к той же группе совместного размещения, в возможно меньшем числе томов.
Узел	Сервер размещает данные узла на как можно меньшем числе томов.	Сервер размещает данные узла на как можно меньшем числе томов.
File space	Сервер размещает данные узла на как можно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах	Сервер сохраняет данные для файловых пространств в возможно меньшем числе томов. Если узел имеет несколько файловых пространств, сервер сохраняет их данные на разных томах

Процедура

Решая, стоит ли и как именно осуществлять совместное размещение данных, сделайте следующее:

1. Определите, как следует организовать данные: на основе узлов клиентов, на основе группы узлов клиентов или на основе файловых пространств. Для совместного размещения по группам нужно решить, как сгруппировать узлы:
   - Если целью является экономия пространства, объединение маленьких узлов в одну группу позволит экономнее использовать ленты.
   - Если целью является потенциальное ускорение клиентских операций восстановления, сгруппируйте вместе узлы, чтобы они заполняли максимально возможное число лент, Если сгруппировать узлы вместе, данные отдельных узлов будут распределены по двум или более лентам и одновременно можно будет смонтировать больше лент во время операции восстановления без запроса в нескольких сеансах.
   - Если целью является разделение данных по отделам, можно группировать узлы по отделам.
2. Чтобы произвести совместное размещение групп, выполните следующие шаги:
   a. Задайте группы совместного размещения с помощью команды DEFINE COLLOCGROUP.
   b. Добавьте в группы совместного размещения клиентские узлы с помощью команды DEFINE COLLOCMEMBER.

   В организации совместного размещения на уровне групп вам помогут следующие запросы:

   QUERY COLLOCGROUP
   : Показывает группы совместного размещения, заданные на сервере.

   QUERY NODE
   : Позволяет вызвать на экран имя группы совместного размещения, к которой принадлежит заданный узел.

   QUERY NODEDATA
   : Позволяет вызвать на экран информацию о данных для одного или более узлов в пуле хранения с последовательным доступом.

QUERY STGPOOL
: Позволяет вызвать на экран информацию о размещении клиентских данных в пуле хранения с последовательным доступом и объеме пространства, занятого на томе данными одного узла.

Также можно использовать сценарии сервера IBM Spectrum Protect или сценарии PerlL, чтобы увидеть информацию, которая может оказаться полезной при создании определений групп совместного размещения.

3. Укажите, как следует производить совместное размещение данных в пуле хранения, введя команду DEFINE STGPOOL или UPDATE STGPOOL с параметром COLLOCATE.

Дальнейшие действия

Подсказка: Чтобы сократить число операций монтирования носителей, более эффективно использовать пространство на последовательных томах и включить совместное размещение, выполните следующие шаги:

- Определить иерархию пулов хранения и политику с требованием, чтобы эти резервные, архивные файлы и файлы с управлением пространством изначально хранились в дисковых пулах хранения.

  Осуществляя перенос данных из дискового пула хранения, сервер выбирает клиентский узел или группу совместного размещения, данные которых занимают в этом пуле хранения больше всего пространства, и пытается перенести все файлы этого узла или группы. Этот процесс хорошо совместим с функцией совместного размещения, поскольку сервер старается поместить все файлы конкретного клиента или их группы на один том с последовательным доступом.

- Разрешите для пула хранения с последовательным доступом использование чистых томов, чтобы сервер мог выбирать новые тома для совместного размещения данных.
- Задайте клиентскую опцию COLLOCATEBYFILESPEC, чтобы ограничить количество лент, на которые записываются объекты, связанные с одной спецификацией файла. Эта опция позволяет более эффективно осуществлять совместное размещение на уровне серверов; она не заменяет установку совместного размещения на уровне файловых пространств или групп.

Управление ленточными устройствами

Стандартные операции с лентами включают подготовку ленточных томов для использования, управления, как и когда тома используются снова, и обеспечение, что доступно достаточно томов. Надо также отвечать на запросы, адресованные оператору, и управлять библиотеками, накопителями, дисками, путями и устройствами перемещения данных.

- Подготовка сменных носителей
  Прежде чем съемный носитель можно будет использовать для хранения данных, его надо подготовить. Стандартные операции подготовки включают определение меток томов и регистрацию томов.
- Управление перечнем томов
  Перечнем томов можно управлять, контролируя доступ сервера к томам, повторно используя ленты, а также повторно используя тома для операций резервного копирования базы данных и экспорта. Перечнем также можно управлять, поддерживая запас чистых томов.
- Частично записанные тома
  Частично записанные тома всегда считаются закрытыми, даже если до их выбора сервером для монтирования они находились в состоянии чистых томов. Сервер отслеживает исходное состояние чистых томов и может вернуть им чистое состояние, когда они станут пустыми.
- Операции с совместно используемыми библиотеками
  Совместно используемые библиотеки - это логические библиотеки, представленные физически библиотеками SCSI. Физическая библиотека управляется сервером IBM Spectrum Protect, настроенным как менеджер библиотеки. Серверы IBM Spectrum Protect, на которых используется тип библиотек SHARED, являются клиентами библиотеки по отношению к серверу менеджера библиотеки IBM Spectrum Protect.
- Управление серверными запросами на тома
  IBM Spectrum Protect показывает требования и сообщения о состоянии во всех клиентах командой строки администрирования, запущенных в режиме консоли. Часто эти запросы ограничены по времени. Успешные операции сервера должны быть выполнены в рамках заданного предела времени; в противном случае произойдет тайм-аут операции.

Подготовка сменных носителей

Прежде чем съемный носитель можно будет использовать для хранения данных, его надо подготовить. Стандартные операции подготовки включают определение меток томов и регистрацию томов.

Об этой задаче

Когда IBM Spectrum Protect обращается к тому на сменном носителе, он проверяет имя тома в заголовке его метки, чтобы гарантировать получение доступа к нужному тому.

Ленточным томам следует присваивать метки для того, чтобы сервер мог их использовать.

Процедура

Чтобы подготовить том для использования, выполните следующие действия:

1. Присвойте метку тому, используя команду LABEL LIBVOLUME.
2. При использовании автоматизированных библиотек необходимо включить том в библиотеку. Инструкции смотрите в разделе Регистрация томов в автоматизированной библиотеке,
   Подсказка: При использовании команды LABEL LIBVOLUME с накопителями автоматизированной библиотеки можно снабдить тома метками и включить их в библиотеку одной командой.
3. Если данный пул хранения не может содержать чистых томов (`MAXSCRATCH=0`), то определите том для IBM Spectrum Protect по имени, чтобы позже к нему можно было осуществлять доступ.

   Если пул хранения может содержать чистые тома (для параметра MAXSCRATCH указано значение, не равное нулю), то пропустите это шаг.

- Запись меток томов на ленточных томах
  Ленточные тома следует снабжать метками до их определения для сервера.
- Регистрация томов в автоматизированной библиотеке
  Вы можете активировать том в автоматизированной библиотеке, используя команду CHECKIN LIBVOLUME.

Запись меток томов на ленточных томах

Ленточные тома следует снабжать метками до их определения для сервера.

Об этой задаче

Для автоматизированных библиотек выводится приглашение вставить том в слот входа/выхода библиотеки. Если доступной станции ввода-вывода нет, то вставьте том в пустой слот. Томам можно присвоить метки, когда вы их будете активировать или до их активирования.

Процедура

Чтобы присвоить томам метки до их активации, выполните следующие шаги:

1. Присвойте метки ленточным томам, используя команду LABEL LIBVOLUME. Например, чтобы присвоить имя VOLUME1 тому в библиотеке LIBRARY 1, введите следующую команду:

   ```
   label libvolume library1 volume1
   ```

   Требование: Должен быть доступен хотя бы один накопитель. Накопитель не может использоваться другим процессом IBM Spectrum Protect. Если том бездействует, то накопитель считается недоступным.
2. Чтобы перезаписать существующие метки томов, укажите параметр `OVERWRITE=YES`. По умолчанию команда LABEL LIBVOLUME не перезаписывает текущую метку тома.

- Запись меток томов в SCSI библиотека (library)
  Томам можно присваивать метки по отдельности, или можно использовать IBM Spectrum Protect, чтобы произвести поиск томов в библиотеке и присвоить метки найденным томам.

Задачи, связанные с данной:
Присвоение меток новым томам с использованием AUTOLABEL
Ссылки, связанные с данной:
LABEL LIBVOLUME (запись метки на том библиотеки)

Регистрация томов в автоматизированной библиотеке

Вы можете активировать том в автоматизированной библиотеке, используя команду CHECKIN LIBVOLUME.

Прежде чем начать

Чтобы автоматически присвоить лентам метки до их активации, введите команду DEFINE LIBRARY, задав параметр AUTOLABEL=YES. Используя параметр AUTOLABEL, вы избежите необходимости предварительно задавать метку для набора лент.

Об этой задаче

Каждый том, используемый сервером в каких бы то ни было целях, должен иметь уникальное имя. Это требование относится ко всем томам, независимо от того, используются ли они для пулов хранения или таких операций, как экспорт или резервное копирование базы данных. Требование относится также к томам, находящимся в разных библиотеках, но используемых одним сервером.

Советы:

- Не используйте одну библиотеку для томов со штрих-кодовыми метками и томов, у которых нет таких меток. Сканирование штрих-кодов может занять длительное время для непомеченных томов.
- Для сервера допустимы только ленты со стандартными метками IBM®.
- Все тома, штрих-код которых начинается с `CLN`, рассматриваются как чистящая лента.
- Если для тома есть запись в файле хронологии, его нельзя зарегистрировать как чистый том.

Процедура

1. Чтобы активировать том хранения в библиотеке, введите команду CHECKIN LIBVOLUME.
   Совет: Команда всегда выполняется как фоновый процесс. Дождитесь завершения выполнения процесса CHECKIN LIBVOLUME, прежде чем задавать тома, иначе этот процесс завершится неудачно. Можно сэкономить время, выполняя регистрацию томов как часть операции маркировки.
2. Присвойте библиотеке имя и укажите, является ли том закрытым или чистым. В зависимости от используемых томов (чистые или закрытые) выполните одно из следующих действий.
   - Если используются только чистые тома, убедитесь в доступности достаточного количества чистых томов. Например, может потребоваться пометить дополнительные тома. Кроме того, после начала использования томов может понадобиться увеличить количество чистых томов, разрешенных для использования пулом хранения, определенным для данной библиотеки.
   - Если в библиотеке необходимо использовать закрытые тома в дополнение к чистым томам или вместо них, задайте тома в пуле хранения, используя команду DEFINE VOLUME. Вы должны пометить и активировать заданные вами тома.

- Активация одного тома в библиотеке SCSI
  Можно активировать один том, введя команду CHECKIN LIBVOLUME и задав параметр SEARCH=NO. IBM Spectrum Protect попросит оператора монтирования загрузить том во входной/выходной слот в библиотеке.
- Регистрация томов в слотах хранения библиотеки
  Если у вас много томов, которые нужно активировать, и вы не хотите вводить команду CHECKIN LIBVOLUME для каждого тома, вы можете произвести поиск слотов хранения для новых томов. Сервер найдет тома, которые еще не были добавлены в перечень.
- Активация томов со входных и выходных портов библиотеки
  Вы можете произвести поиск промаркированных томов во всех слотах входных и выходных портов, и сервер может активировать их автоматически.
- Активация томов с использованием устройств чтения штрих-кода
  При активации томов в библиотеках, снабженных устройствами чтения штрих-кода, можно сэкономить время, используя символы на этикетках со штрих-кодом в качестве имен томов.
- Регистрация томов с использованием устройств чтения штрих-кода
  Вы сможете сэконосить время при активации томов, используя устройство чтения штрих-кода, если оно есть в библиотеке.
- Активация томов в полной библиотеке с заменой
  Если при активации томов в библиотеке отсутствуют пустые слоты, то активация завершится неудачно, если не будет разрешена *замена* томов. Если вы включите замену, а библиотека окажется заполнена, сервер выберет том, который нужно извлечь, а затем активирует затребованный вами том.

- Операционные системы WindowsЗакрытые и чистые тома
  Чтобы оптимизировать хранение на ленте, прочтите информацию о закрытых томах и чистых томах. Используйте закрытые тома и чистые тома соответствующим образом.
- Операционные системы WindowsАдреса элементов для слотов хранения в библиотеке
  Адрес элемента — это номер, который указывает физическое размещение слота хранилища или накопителя в автоматизированной библиотеке.

Задачи, связанные с данной:
Запись меток томов на ленточных томах

Активация одного тома в библиотеке SCSI

Можно активировать один том, введя команду CHECKIN LIBVOLUME и задав параметр SEARCH=NO. IBM Spectrum Protect попросит оператора монтирования загрузить том во входной/выходной слот в библиотеке.

Процедура

1. Введите команду CHECKIN LIBVOLUME.

   Например, чтобы активировать том VOL001, введите следующую команду:

   ```
   checkin libvolume tapelib vol001 search=no status=scratch
   ```

2. Отреагируйте на подсказку с сервера.
   - Если библиотека имеет порт входа/выхода, то выводится приглашение вставить ленту в порт входа/выхода.
   - Если библиотека не имеет порта входа/выхода, то выводится приглашение вставить ленту в один из слотов библиотеки. Адреса элементов позволяют идентифицировать эти слоты. Например, сервер обнаруживает, что первый пустой слот - это слот с адресом элемента, равным 5. В этом случае сообщение будет выглядеть следующим образом:

     ```
     ANR8306I 001: Вставьте том 8MM VOL001 R/W в слот с адресом элемента
     5 библиотеки TAPELIB в течение 60 минут; введите команду 'REPLY' вместе
     с идентификатором запроса, когда будете готовы.
     ```

     Если вы не знаете, где находится в библиотеке элемент с адресом 5, смотрите рабочую таблицу для устройства. Чтобы найти рабочую таблицу, смотрите документацию по вашей библиотеке. Вставив том (в ответ на соответствующее предложение), ответьте на сообщение от клиента администрирования IBM Spectrum Protect. Введите команду REPLY, указав после нее номер требования (номер в начале требования о монтировании), например:

     ```
     reply 1
     ```

     Совет: Иногда адреса элементов нумеруются, начиная с номера, отличного от единицы. Чтобы точно узнать нумерацию, смотрите рабочую таблицу. Если на сайте IBM® для IBM Spectrum Protect отсутствует рабочая таблица для вашего устройства, смотрите документацию по вашей библиотеке.

   Если вы зададите время ожидания, равное 0, используя дополнительный параметр WAITTIME в команде CHECKIN LIBVOLUME, команда REPLY не потребуется. Время ожидания по умолчанию составляет 60 минут.

Регистрация томов в слотах хранения библиотеки

Если у вас много томов, которые нужно активировать, и вы не хотите вводить команду CHECKIN LIBVOLUME для каждого тома, вы можете произвести поиск слотов хранения для новых томов. Сервер найдет тома, которые еще не были добавлены в перечень.

Процедура

1. Откройте библиотеку и поместите новые тома в неиспользуемые слоты. Например, в случае устройства SCSI откройте дверцу библиотеки, вставьте все новые тома в незанятые слоты и закройте дверцу.
2. Если томам не присвоены метки, используйте команду LABEL LIBVOLUME, чтобы присвоить тому метку.
3. Выполните команду CHECKIN LIBVOLUME с параметром SEARCH=YES.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Активация томов со входных и выходных портов библиотеки

Вы можете произвести поиск промаркированных томов во всех слотах входных и выходных портов, и сервер может активировать их автоматически.

Прежде чем начать

Введите команду LABEL LIBVOLUME, чтобы присвоить метки томам, у которых их еще нет.

Об этой задаче

При работе с библиотеками SCSI сервер проверяет все порты входа/выхода библиотеки на наличие томов. При обнаружении тома с действительной меткой он активируется автоматически.

Процедура

Введите команду CHECKIN LIBVOLUME с параметром SEARCH=BULK.

- Чтобы загрузить ленту в накопитель и прочитать метку, задайте параметр CHECKLABEL=YES. После того как сервер прочитает метку, он переместит ленту из накопителя в слот хранения.
- Чтобы сервер использовал устройство для чтения штрих-кода для проверки внешних меток на лентах, задайте параметр CHECKLABEL=BARCODE. Когда включено чтение штрих-кода, сервер читает метку и перемещает ленту со входного/выходного порта в слот хранения.

Активация томов с использованием устройств чтения штрих-кода

При активации томов в библиотеках, снабженных устройствами чтения штрих-кода, можно сэкономить время, используя символы на этикетках со штрих-кодом в качестве имен томов.

Об этой задаче

Сервер читает метки со штрих-кодом и использует эту информацию для записи внутренних меток носителей. В случае томов, у которых нет этикеток со штрих-кодом, сервер монтирует тома в накопитель и пытается прочитать внутреннюю записанную метку.

Процедура

Введите команду CHECKIN LIBVOLUME с параметром CHECKLABEL=BARCODE. Например, чтобы с помощью устройства считывания штрих-кода выполнить поиск в библиотеке с именем TAPELIB и зарегистрировать чистую ленту, введите следующую команду:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Регистрация томов с использованием устройств чтения штрих-кода

Вы сможете сэконосить время при активации томов, используя устройство чтения штрих-кода, если оно есть в библиотеке.

Об этой задаче

При активации тома можно указать, надо ли считывать метки носителей во время активации. Если проверка метки включена, IBM Spectrum Protect монтирует каждый том, чтобы считать внутреннюю метку, и активирует том, только если он должным образом помечен. Проверка меток поможет в будущем предотвратить ошибки, когда тома будут использоваться в пулах хранения, но при этом время обработки регистрации увеличивается.

Если том не имеет этикетки со штрих-кодом, то IBM Spectrum Protect монтирует его в накопитель и пытается считать записанную метку.

Процедура

Чтобы активировать тома, используя устройство считывания штрих-кода, введите команду CHECKIN LIBVOLUME, задав параметр CHECKLABEL=BARCODE. Например, чтобы с помощью устройства считывания штрих-кода активировать все тома как чистые тома в библиотеке TAPELIB, введите следующую команду:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Задачи, связанные с данной:
Подготовка сменных носителей
Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Активация томов в полной библиотеке с заменой

Если при активации томов в библиотеке отсутствуют пустые слоты, то активация завершится неудачно, если не будет разрешена *замена* томов. Если вы включите замену, а библиотека окажется заполнена, сервер выберет том, который нужно извлечь, а затем активирует затребованный вами том.

Об этой задаче

Сервер выберет том, который нужно извлечь, проверив сначала наличие любого доступного чистого тома, а затем тома, который монтировался реже других. Сервер удалит выбранный для замены том из библиотеки и заменит его томом, который вы активируете.

Процедура

Чтобы заменять тома, если пустой слот библиотеки недоступен для активации тома, введите команду CHECKIN LIBVOLUME, задав параметр SWAP=YES. Например, чтобы активировать том с именем `VOL1` в библиотеке AUTO и задать замену, введите следующую команду:

```
checkin libvolume auto vol1 swap=yes
```

Задачи, связанные с данной:
Управление заполненной библиотекой с хранилищем переполнения
Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Закрытые и чистые тома

Чтобы оптимизировать хранение на ленте, прочтите информацию о закрытых томах и чистых томах. Используйте закрытые тома и чистые тома соответствующим образом.

Закрытые тома не могут быть перезаписаны, если запрошено монтирование чистых томов. Активировать том в состоянии Чистый нельзя, если этот том используется пулом хранения для экспорта данных, для резервного копирования базы данных или для резервного копирования на том набора резервных копий.

Частично записанные тома всегда являются закрытыми. Тома имеют состояние либо чистых, либо закрытых, но когда IBM Spectrum Protect сохраняет на них данные, их состояние становится закрытым.

Табл. 1. Использование закрытых томов и чистых томов

Тип тома	**Когда следует использовать**
Закрытые тома	Используйте закрытые тома, чтобы контролировать тома, используемые отдельными пулами хранения, и вручную управлять томами. Чтобы задать закрытые тома, введите команду DEFINE VOLUME. Для восстановления базы данных, дампа памяти или загрузки, а также для серверных операций импорта нужно указать закрытые тома.

Тип тома	Когда следует использовать
Свободные тома	В некоторых случаях можно упростить управление томами, используя чистые тома. Чистые тома можно использовать в следующих случаях: • Когда не нужно описывать каждый том в пуле хранения. • Если вы хотите воспользоваться преимуществами автоматизации роботизированных устройств. • Когда разные пулы хранения совместно используют автоматизированную библиотеку, и пулы хранения могут динамически получить тома из чистых томов в библиотеке. Предварительно распределять тома по пулам хранения не требуется.

Задачи, связанные с данной:
Изменение состояния тома в автоматизированной библиотеке
Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
DELETE VOLUME (удаление тома пула хранения)

Адреса элементов для слотов хранения в библиотеке

Адрес элемента — это номер, который указывает физическое размещение слота хранилища или накопителя в автоматизированной библиотеке.

Если в библиотеке есть входные/выходные порты, вы можете добавлять и удалять носители, используя порты. Если никаких входных/выходных портов нет, вы должны будете загрузить ленты в слоты хранения.

Если вы загружаете ленточные носители в слоты хранения, вы должны должны будете реагировать на запросы о монтировании, в которых слоты хранилища будут указаны в виде адресов элементов. Если при вводе команды CHECKIN LIBVOLUME или LABEL LIBVOLUME вы не задали нулевое время ожидания, вам не нужно будет реагировать на требование монтирования.

Адреса элементов смотрите в документации производителя устройства или перейдите на сайт IBM® для IBM Spectrum Protect и произведите поиск адресов элементов.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
LABEL LIBVOLUME (запись метки на том библиотеки)

Управление перечнем томов

Перечнем томов можно управлять, контролируя доступ сервера к томам, повторно используя ленты, а также повторно используя тома для операций резервного копирования базы данных и экспорта. Перечнем также можно управлять, поддерживая запас чистых томов.

Об этой задаче

Каждый том, использующийся сервером, должен иметь уникальное имя, независимо от того, используются ли они для пулов хранения или таких операций, как экспорт или резервное копирование базы данных. У томов, находящихся в разных библиотеках, но используемых одним и тем же сервером, также должны быть уникальные имена.

- Управление доступом к томам
  Для управления доступом к томам можно использовать разные методы.
- Повторное использование лент
  Чтобы поддерживать необходимый запас лент, вы можете производить удаление устаревших файлов, освобождать тома и удалять тома, срок службы которых подошел к концу. Вы также можете держать в запасе чистые тома.
- Поддержание запаса чистых томов.
  Вы должны задать для пула хранения достаточно большое максимальное число чистых томов в соответствии с

ожидаемым уровнем использования.

- Операционные системы AIX Операционные системы LinuxПоддержание запаса томов в библиотеке, содержащей носители WORM
  Предотвращайте отмену транзакций сохранения данных в библиотеках, содержащих тома с однократной записью и многократным чтением (Write-Once, Read-Many, WORM), поддерживая запас чистых или новых закрытых томов в библиотеке. Отмена транзакций может привести к бесполезному расходованию носителей WORM.
- Управление перечнем томов в автоматизированных библиотеках
  Сервер IBM Spectrum Protect использует перечень томов библиотеки для отслеживания чистых и закрытых томов, которые есть в автоматизированной библиотеке. Вы должны убедиться, что перечень соответствует томам, которые физически находятся в библиотеке.

Управление доступом к томам

Для управления доступом к томам можно использовать разные методы.

Процедура

Чтобы управлять доступом к томам, выполните любое из следующих действий:

- Чтобы запретить серверу монтировать том, введите команду UPDATE VOLUME и задайте параметр ACCESS=UNAVAILABLE.
- Чтобы сделать тома недоступными и отправить их куда-либо вне сайта для защиты, используйте пул хранения копий или пул хранения активных данных.
- Можно создать резервные копии первичных пулов хранения, после чего отправить тома пула хранения копий в дистанционное хранилище.
- Можно скопировать активные версии клиентских резервных данных в пулы хранения активных данных, а затем отправить тома в хранилище, расположенное вне узла.
- Отслеживать тома пула хранения копий и пула активных данных можно путем изменения режима доступа к ним на дистанционное хранилище, а также путем обновления журнала томов для определения их расположения.

Ссылки, связанные с данной:
UPDATE VOLUME (изменение тома пула хранения)

Повторное использование лент

Чтобы поддерживать необходимый запас лент, вы можете производить удаление устаревших файлов, освобождать тома и удалять тома, срок службы которых подошел к концу. Вы также можете держать в запасе чистые тома.

Об этой задаче

Со временем носители устаревают, а размещенные на них резервные копии данных становятся ненужными. Можно задать политики сервера, определяющие количество версий резервных копий и срок их хранения. Можно использовать обработку устаревания, чтобы удалять файлы, которые вам больше не нужны. Нужные вам данные можно оставить на носителе. Когда данные станут вам больше не нужны, вы сможете высвободить носители и использовать их повторно.

Процедура

1. Удаляйте ненужные данные клиента, регулярно выполняя обработку устаревания. При обработке устаревания удаляются данные, которые устарели либо в результате превышения срока хранения, указанного в политике, либо потому, что администратор удалил активные версии данных.
2. Повторно используйте тома в пулах хранения, выполняя обработку высвобождения.

   В процессе обработки высвобождения носителей все не устаревшие данные консолидируются путем перемещения с многих томов на меньшее количество томов. После этого носители могут быть возвращены в пул хранения и использованы повторно.

3. Повторно используйте тома, содержащие устаревшие резервные копии базы данных или ненужные экспортированные данные, удаляя хронологию томов.

   Прежде чем сервер сможет повторно использовать тома, отслеживаемые в файле хронологии томов, вы должны удалить информацию о томе из файла хронологии томов, введя команду DELETE VOLHISTORY.

Совет: Если сервер использует disaster recovery manager (DRM), то информация о томах удаляется автоматически во время обработки команды MOVE DRMEDIA.

4. Определяйте, какие ленточные тома достигают окончания срока использования. Сервер можно использовать для вывода статистики томов, включающей в себя число операций записи, выполненных на носитель, и число ошибок записи. Для закрытых и чистых томов будут показаны следующие статистические данные:

   Закрытые тома
   : Для носителей, изначально определенных как закрытые тома, сервер сохраняет статистические данные, даже когда том высвобождается. Эту информацию можно сравнить с количеством операций записи и ошибок записи, рекомендованным производителем.

   Свободные тома
   : Для носителей, изначально определенных в качестве чистых томов, сервер обновляет статистические данные при каждом освобождении томов.

5. Следует восстановить все действительные данные с томов, достигших окончания срока использования. Если тома находятся в автоматизированных библиотеках, следует отменить их регистрацию в перечне библиотеки. Удалите закрытые тома из базы данных при помощи команды DELETE VOLUME.
6. Убедитесь, что тома доступны для ротации лент, и пулу хранения не грозит нехватка пространства. Для мониторинга доступности чистых томов можно использовать Центр операций. Убедитесь, что число чистых томов достаточно велико, чтобы соответствовать требованиям. Дополнительную информацию смотрите в разделе Поддержание запаса томов в библиотеке, содержащей носители WORM.
   носитель WORM: Накопители однократной записи и многократного чтения (Write Once Read Many, WORM) при отмене сервером транзакций могут зря расходовать носители, поскольку тома становятся недоступными для выполнения резервного копирования. После того, как сервер произведет запись на тома WORM, пространство на томе нельзя будет использовать повторно, даже если транзакции были отменены (например, при отмене резервного копирования из-за недостаточного числа носителей в устройстве). Чтобы свести к минимуму бесполезное расходование носителей WORM, сделайте следующее:
   a. Убедитесь, что максимальное количество чистых томов для пула хранения устройства как минимум равно количеству слотов хранилища в библиотеке.
   b. Зарегистрируйте в перечне томов устройства достаточное количество томов для ожидаемой загрузки.

   Если большинство операций резервного копирования предназначено для небольших файлов, то управление размером транзакций может повлиять на использование дисков WORM. Чем меньше операция, тем меньшее количество места становится непригодным в случае отмены операции (например, резервного копирования). Размеры операций управляются серверным параметром TXNGROUPMAX и клиентским параметром TXNBYTELIMIT.

Задачи, связанные с данной:
Перенос данных на обновленные накопители
Управление серверными запросами на тома
Ссылки, связанные с данной:
DELETE VOLHISTORY (Удалить информацию хронологии томов с последовательным доступом)
DELETE VOLUME (удаление тома пула хранения)
Опция Txnbytelimit
опция сервера TXNGROUPMAX
Информация, связанная с данной:
EXPIRE INVENTORY (ручной запуск обработки устаревания перечня)
RECLAIM STGPOOL (консолидация томов пула хранения с последовательным доступом)

Поддержание запаса чистых томов.

Вы должны задать для пула хранения достаточно большое максимальное число чистых томов в соответствии с ожидаемым уровнем использования.

Об этой задаче

При задании пула хранения необходимо указать максимальное число свободных томов, которые может использоваться в пуле хранения. Сервер при необходимости запрашивает свободный том автоматически. Если число чистых томов, используемых сервером для пула хранения, превысит заданный максимум, это может привести к нехватке пространства в пуле хранения.

Процедура

Если пулу хранения потребуется число чистых томов, превышающее максимальное, можно выполнить одно из указанных ниже действий или оба эти действия:

1. Увеличьте максимальное количество чистых томов, введя команду UPDATE STGPOOL с параметром MAXSCRATCH.
2. Сделать тома доступными для повторного использования, запустив обработку устаревания и высвобождения томов, чтобы собрать данные на меньшем числе томов.
    a. Введите команду EXPIRE INVENTORY, чтобы запустить обработку устаревания.
    Совет: По умолчанию этот процесс автоматически запускается каждый день. В файле серверных опций, dsmserv.opt, также можно задать серверную опцию EXPINTERVAL, чтобы автоматически запустить обработку устаревания. Значение, равное 0, указывает, что для запуска обработки устаревания нужно ввести команду EXPIRE INVENTORY.
    b. Введите команду RECLAIM STGPOOL, чтобы запустить обработку высвобождения пространства.
    Совет: Вы также можете задать пороги высвобождения пространства, когда будете задавать пул хранения с использованием команды DEFINE STGPOOL с параметром RECLAIMPROCESS.

Дальнейшие действия

Если вам потребуется больше томов для будущих операций восстановления, присвойте метки дополнительным чистым томам, используя команду LABEL LIBVOLUME.

Задачи, связанные с данной:

Поддержание запаса чистых томов в автоматизированной библиотеке

Ссылки, связанные с данной:

LABEL LIBVOLUME (запись метки на том библиотеки)

UPDATE STGPOOL (обновить пул хранения)

Информация, связанная с данной:

EXPIRE INVENTORY (ручной запуск обработки устаревания перечня)

RECLAIM STGPOOL (консолидация томов пула хранения с последовательным доступом)

Поддержание запаса томов в библиотеке, содержащей носители WORM

Предотвращайте отмену транзакций сохранения данных в библиотеках, содержащих тома с однократной записью и многократным чтением (Write-Once, Read-Many, WORM), поддерживая запас чистых или новых закрытых томов в библиотеке. Отмена транзакций может привести к бесполезному расходованию носителей WORM.

Об этой задаче

IBM Spectrum Protect отменяет транзакцию, если тома - закрытые или чистые - недоступны для завершения операции сохранения данных. После того как IBM Spectrum Protect начнет транзакцию, производя запись на том WORM, записанное на нем пространство нельзя будет использовать повторно даже в случае отмены транзакции.

Например, у вас есть тома WORM по 2,6 ГБ каждый, и клиент запустит резервное копирование файла объемом 12 ГБ. Если IBM Spectrum Protect не может после заполнения четырех чистых томов получить пятый, то операция резервного копирования отменяется. Четыре тома, которые IBM Spectrum Protect уже заполнил данными, не могут использоваться повторно.

Чтобы свести к минимуму отмену транзаций, в библиотеке должно быть достаточно доступных томов для выполнения ожидаемых операций клиентов (например, резервного копирования).

Процедура

1. Убедитесь, что в пуле хранения, связанном с библиотекой, достаточно чистых томов. Введите команду UPDATE STGPOOL, задав параметр MAXSCRATCH.
2. Чтобы управлять ожидаемой нагрузкой, активируйте в библиотеке достаточное количество чистых и закрытых томов, введя команду CHECKIN LIBVOLUME.
3. Чтобы управлять размером транзакций, задайте опцию сервера TXNGROUPMAX и опцию клиента TXNBYTELIMIT. Если клиент чаще сохраняет небольшие файлы, управление размером транзакций может повлиять на то, как используются тома WORM. Чем меньше транзакция, тем меньше пространства хранения будет израсходовано напрасно в случае отмены операции (например, резервного копирования).

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
UPDATE STGPOOL (обновить пул хранения)
Опция Txnbytelimit
опция сервера TXNGROUPMAX

Управление перечнем томов в автоматизированных библиотеках

Сервер IBM Spectrum Protect использует перечень томов библиотеки для отслеживания чистых и закрытых томов, которые есть в автоматизированной библиотеке. Вы должны убедиться, что перечень соответствует томам, которые физически находятся в библиотеке.

Инвентарный список томов библиотеки отделен от инвентарного списка томов для каждого пула хранения. Чтобы добавить том в перечень томов библиотеки, вы активируете том в этой библиотеке IBM Spectrum Protect.

Список томов в перечне томов библиотеки может не совпадать со списком томов в перечне пулов хранения для устройства. Например, можно активировать чистые тома в библиотеке, но их нельзя будет задать в пуле хранения. Если чистые тома не выбраны для резервного копирования, то вы сможете задать закрытые тома в пуле хранения, но не сможете активировать их в перечне томов для устройства.

Чтобы перечень томов для библиотеки сервера оставался точным, зарезервируйте тома, чтобы физически удалить тома из библиотеки SCSI. Если попытаться зарезервировать том, который используется в пуле хранения, том останется в пуле хранения. Если вы должны смонтировать том, когда он зарезервирован, на консоли оператора монтирования появится сообщение с требованием активировать том. Если операция активации завершится неудачно, сервер пометит том как недоступный.

Если том присутствует в перечне томов библиотеки, его можно перевести из состояния чистого в состояние закрытого.

Чтобы проверить, согласуется ли перечень томов библиотеки сервера с томами, физически находящимися в библиотеке, можно произвести аудит библиотеки. Перечень может стать неточным, если тома помещаются к библиотеку или удаляются из нее без передачи соответствующих сведений на сервер с помощью команд check-in или check-out.

- Изменение состояния тома в автоматизированной библиотеке
  Вы можете изменить состояние тома с private (закрытый) на scratch (чистый) или наоборот.
- Удаление томов из автоматизированной библиотеки
  Тома можно удалить из автоматизированной библиотеки, если вы экспортировали данные на том и хотите импортировать данные в другую систему. Вам также может потребоваться удалить тома, чтобы освободить место для новых томов.
- Поддержание запаса чистых томов в автоматизированной библиотеке
  Задавая пул хранения, связанный с автоматизированной библиотекой, вы можете указать максимальное число чистых томов, равное физической емкости библиотеки. Если сервер использует для пула хранения большее число чистых томов, вы должны убедиться, что у вас есть достаточное число доступных томов.
- Управление заполненной библиотекой с хранилищем переполнения
  С ростом потребности в пространстве хранения число томов, необходимых в пуле хранения, может превысить физическую емкость автоматизированной библиотеки. Чтобы сделать пространство доступным для новых томов и чтобы отслеживать существующие тома, можно задать хранилище переполнения для пула хранения.
- Аудит перечня томов в библиотеке
  Можно выполнить аудит автоматизированной библиотеки, чтобы обеспечить соответствие инвентарного списка томов библиотеки и томов, которые физически в ней находятся. Можно выполнить аудит библиотеки в случае нарушения целостности перечня томов библиотеки из-за перемещения томов в библиотеке вручную или в связи с ошибками базы данных.

Задачи, связанные с данной:
Регистрация томов в автоматизированной библиотеке
Ссылки, связанные с данной:
AUDIT LIBRARY (аудит томов автоматизированной библиотеки)

Изменение состояния тома в автоматизированной библиотеке

Вы можете изменить состояние тома с private (закрытый) на scratch (чистый) или наоборот.

Процедура

Чтобы изменить состояние тома, введите команду UPDATE LIBVOLUME. Например, чтобы изменить состояние тома с именем VOL1 на частный том, введите следующую команду:

```
update libvolume lib1 vol1 status=private
```

Ограничения:

- Если том принадлежит к пулу хранения или указан в файле хронологии томов, изменить состояние тома с закрытого на чистый нельзя.
- Закрытые тома должны представлять собой заданные администратором тома, на которых либо нет никаких данных, либо содержатся недействительные данные. Это не могут быть частично записанные тома, содержащие активные данные. При изменении состояния статистика тома теряется.

Удаление томов из автоматизированной библиотеки

Тома можно удалить из автоматизированной библиотеки, если вы экспортировали данные на том и хотите импортировать данные в другую систему. Вам также может потребоваться удалить тома, чтобы освободить место для новых томов.

Об этой задаче

По умолчанию сервер монтирует зарезервировоанный том и проверяет внутреннюю метку. При проверке метки сервер удаляет том из инвентарного списка томов библиотеки, а затем перемещает его на порт входа/выхода или на станцию ввода-вывода библиотеки. Если в библиотеке нет порта входа/выхода, то сервер выдает оператору монтирования запрос на удаление тома из слота в библиотеке.

Процедура

- Чтобы удалить том из автоматической библиотеки, введите команду CHECKOUT LIBVOLUME.
- Для автоматизированных библиотек с несколькими портами ввода/выхода введите команду CHECKOUT LIBVOLUME с параметром REMOVE=BULK. Сервер извлечет том к следующему доступному порту ввода/выхода.

Дальнейшие действия

Если вы резервируете том, заданный в пуле хранения, а серверу потребуется потом получить к нему доступ, то сервер затребует активацию тома. Чтобы возвратить тома в библиотеку, введите команду CHECKIN LIBVOLUME.

Ссылки, связанные с данной:

CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

CHECKOUT LIBVOLUME (исключение тома хранения из библиотеки)

Поддержание запаса чистых томов в автоматизированной библиотеке

Задавая пул хранения, связанный с автоматизированной библиотекой, вы можете указать максимальное число чистых томов, равное физической емкости библиотеки. Если сервер использует для пула хранения большее число чистых томов, вы должны убедиться, что у вас есть достаточное число доступных томов.

Процедура

Если число чистых томов, которые сервер использует для пула хранения, превысит максимальное число, заданное в определении пула хранения, выполните следующие шаги:

1. Добавьте в библиотеку чистые тома, введя команду CHECKIN LIBVOLUME.
   Совет: Вам может потребоваться хранилище переполнения, чтобы можно было высвободить место для этих чистых томов путем перемещения томов из библиотеки. Дополнительные сведения смотрите в разделе Управление заполненной библиотекой с хранилищем переполнения.
2. Увеличьте максимальное число чистых томов, которые можно добавить в пул хранения, введя команду UPDATE STGPOOL и задав параметр MAXSCRATCH.

Дальнейшие действия

Вам может потребоваться больше томов для будущих операций восстановления, поэтому рассмотрите возможность снабдить метками и выделить несколько дополнительных чистых томов.

Задачи, связанные с данной:
Поддержание запаса чистых томов.

Управление заполненной библиотекой с хранилищем переполнения

С ростом потребности в пространстве хранения число томов, необходимых в пуле хранения, может превысить физическую емкость автоматизированной библиотеки. Чтобы сделать пространство доступным для новых томов и чтобы отслеживать существующие тома, можно задать хранилище переполнения для пула хранения.

Об этой задаче

Сервер отслеживает тома, перемещенные в зону переполнения, и делает слоты хранения доступными для новых томов.

Процедура

1. Создайте хранилище переполнения для томов. Задайте или обновите пул хранения, связанный с автоматизированной библиотекой, при помощи команды DEFINE STGPOOL или UPDATE STGPOOL с параметром OVFLOCATION. Например, чтобы создать хранилище переполнения с именем `ROOM2948` для пула хранения с именем `ARCHIVEPOOL`, введите следующую команду:

   ```
   update stgpool archivepool ovflocation=Room2948
   ```

2. Если вам нужно создать в библиотеке пространство для чистых томов, переместите заполненные тома в хранилище переполнения, введя команду MOVE MEDIA. Например, чтобы переместить все заполненные тома в указанный пул хранения за пределами библиотеки, введите следующую команду:

   ```
   move media * stgpool=archivepool
   ```

3. Активируйте новые чистые тома (если необходимо).
   Ограничение: Если для тома есть запись в файле хронологии тома, то его нельзя зарегистрировать как чистый том. Дополнительную информацию смотрите в разделе Регистрация томов в автоматизированной библиотеке.
4. Определите пустые чистые ленты в хранилище переполнения, введя команду QUERY MEDIA. Например, введите следующую команду:

   ```
   query media * stg=* whereovflocation=Room2948 wherestatus=empty
   ```

5. Если сервер затребует дополнительные тома, найдите и активируйте тома из хранилища переполнения.

   Чтобы найти тома в хранилище переполнения, введите команду QUERY MEDIA. Команду QUERY MEDIA также можно использовать для генерирования команд посредством активации томов.

   Чтобы посмотреть список томов в хранилище переполнения и одновременно сгенерировать команды для активации этих томов в библиотеке, введите примерно следующую команду:

   ```
   query media format=cmd stgpool=archivepool whereovflocation=Room2948
   cmd="checkin libvol autolib &vol status=private"
   cmdfilename="\storage\move\media\checkin.vols"
   ```

   Советы:
   - Требования монтирования от сервера содержат расположение томов.
   - Чтобы задать срок в днях, по истечении которого тома станут подлежать обработке, введите команду UPDATE STGPOOL и задайте параметр REUSEDELAY.
   - Файл, содержащий сгенерированную команду, можно запустить с помощью команды IBM Spectrum Protect MACRO.

Ссылки, связанные с данной:
MOVE MEDIA (перемещение носителей пула хранения с последовательным доступом)
QUERY MEDIA (запрос о носителе пула хранения с последовательным доступом)
UPDATE STGPOOL (обновить пул хранения)

Аудит перечня томов в библиотеке

Можно выполнить аудит автоматизированной библиотеки, чтобы обеспечить соответствие инвентарного списка томов библиотеки и томов, которые физически в ней находятся. Можно выполнить аудит библиотеки в случае нарушения целостности перечня томов библиотеки из-за перемещения томов в библиотеке вручную или в связи с ошибками базы данных.

Процедура

1. Убедитесь, что на накопителях в библиотеке не смонтировано никаких томов. Если есть какие-либо смонтированные тома, которые находятся в состоянии IDLE, введите команду DISMOUNT VOLUME, чтобы их размонтировать.
2. Произведите аудит перечня томов, введя команду AUDIT LIBRARY. Выполните одно из следующих действий.
   - Если у библиотеки есть устройство чтения штрих-кодов, вы можете сэкономить время, воспользовавшись устройством чтения штрих-кодов для идентификации томов. Например, выполнить аудит библиотеки TAPELIB с помощью устройства считывания штрих-кода можно по следующей команде:

     ```
     audit library tapelib checklabel=barcode
     ```

   - Если у библиотеки нет устройства для чтения штрих-кодов, введите команду AUDIT LIBRARY, не задавая параметр CHECKLABEL=BARCODE. Сервер монтирует каждый том, чтобы проверить метку. После проверки метки сервер завершит аудит всех остальных томов.

Результаты

Сервер удаляет из перечня отсутствующие тома и обновляет данные о расположении томов, перемещенных со времени последнего аудита.

Ограничение: Во время аудита сервер не может добавлять тома в перечень.
Задачи, связанные с данной:
Запись меток томов на ленточных томах
Ссылки, связанные с данной:
AUDIT LIBRARY (аудит томов автоматизированной библиотеки)
DISMOUNT VOLUME (Размонтировать том, заданный по имени)

Частично записанные тома

Частично записанные тома всегда считаются закрытыми, даже если до их выбора сервером для монтирования они находились в состоянии чистых томов. Сервер отслеживает исходное состояние чистых томов и может вернуть им чистое состояние, когда они станут пустыми.

Кроме томов в автоматизированных библиотеках, сервер не располагает сведениями о чистом томе до его установки. Затем состояние тома меняется на закрытое, и том автоматически определяется как часть пула хранения, для которого был сделан запрос на монтирование.

Задачи, связанные с данной:
Изменение состояния тома в автоматизированной библиотеке

Операции с совместно используемыми библиотеками

Совместно используемые библиотеки - это логические библиотеки, представленные физически библиотеками SCSI. Физическая библиотека управляется сервером IBM Spectrum Protect, настроенным как менеджер библиотеки. Серверы IBM Spectrum Protect, на которых используется тип библиотек SHARED, являются клиентами библиотеки по отношению к серверу менеджера библиотеки IBM Spectrum Protect.

Клиент библиотеки связывается с диспетчером библиотек, когда запускается диспетчер библиотек и инициализируется устройство хранения, или после определения диспетчера библиотек клиенту библиотеки. Клиент библиотеки подтверждает, что сервер на связи является менеджером библиотеки для указанного библиотечного устройства. Клиент библиотеки также проверяет согласованность определений накопителей с менеджером библиотеки. Клиент библиотеки связывается с менеджером библиотеки для выполнения каждой из следующих операций:

Монтирование тома

Клиент библиотеки посылает менеджеру библиотеки запрос на доступ к определенному тому совместно используемого библиотечного устройства. Для чистого тома клиент библиотеки имя не указывает. Если менеджеру библиотеки не удается получить доступ к запрошенному тому, или если чистые тома недоступны, менеджер отклоняет запрос на монтирование. Если монтирование выполнено успешно, менеджер библиотеки возвращает имя накопителя, в который смонтирован том.

Освобождение тома

Если клиенту библиотеки больше не нужен доступ к тому, он сообщает менеджеру библиотеки, что том можно вернуть в чистое состояние. База данных менеджера библиотеки обновляется значением нового расположения для тома, который теперь находится в перечне библиотечного сервера. Том удаляется из перечня томов клиента библиотеки.

Табл. 1 показывает взаимодействие между клиентами и менеджером библиотеки в процессе обработки операций IBM Spectrum Protect.

Табл. 1. Как серверы, поддерживающие SAN, обрабатывают операции IBM Spectrum Protect

Операция **(команда)**	**Менеджер библиотеки**	**Библиотечный клиент**
Запрос томов библиотеки (QUERY LIBVOLUME)	Показывает тома, зарегистрированные в библиотеке. Для закрытых томов будет также показан сервер-владелец.	Неприменимо.
Регистрация и изъятие томов библиотеки (CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME)	Посылает команды библиотечному устройству.	Неприменимо. Если операция активации должна быть выполнена из-за восстановления клиента, серверу менеджера библиотеки посылается требование.
Перемещение обычных носителей и носителей DRM (MOVE MEDIA, MOVE DRMEDIA)	Допустимо только для томов, используемых сервером менеджера библиотеки.	Запрашивает завершение операции сервером менеджера библиотеки. Вызывает процесс резервирования на сервере менеджера библиотеки.
Аудит перечня библиотеки (AUDIT LIBRARY)	Синхронизирует перечень с библиотечным устройством.	Синхронизирует перечень с сервером менеджера библиотеки.
Маркировка тома библиотеки (LABEL LIBVOLUME)	Помечает и активирует тома.	Неприменимо.
Размонтирование тома (DISMOUNT VOLUME)	Посылает запрос библиотечному устройству.	Запрашивает завершение операции сервером менеджера библиотеки.
Запрос тома (QUERY VOLUME)	Проверяет, владеет ли томом запрашиваемый клиент библиотеки и находится ли этот том в библиотечном устройстве.	Запрашивает завершение операции сервером менеджера библиотеки.

Управление серверными запросами на тома

IBM Spectrum Protect показывает требования и сообщения о состоянии во всех клиентах командой строки администрирования, запущенных в режиме консоли. Часто эти запросы ограничены по времени. Успешные операции сервера должны быть выполнены в рамках заданного предела времени; в противном случае произойдет тайм-аут операции.

Об этой задаче

Для автоматизированных библиотек используйте команды CHECKIN LIBVOLUME и LABEL LIBVOLUME, чтобы вставить картриджи в слоты. Если вы зададите значение параметра WAITTIME, то появится ответное сообщение. Если значение параметра равно нулю, ответ не требуется. Введя команду CHECKOUT LIBVOLUME, вы должны будете вставить картриджи в слоты, и во всех случаях появится ответное сообщение.

Процедура

В следующей таблице представлена информация, как обрабатывать различные задачи для носителей сервера.

Задача	**Подробности**
Использование клиента администрирования при работе с запросами на монтирование	Сервер отправляет сообщения о состоянии запросов на монтирование на серверную консоль и всем клиентам командной строки администрирования, которые были запущены в режиме монтирования или режиме консоли Для запуска клиента командной строки администрирования в режиме монтирования введите команду dsmadmc -mountmode в клиенте командной строки администрирования.
Получение сообщений об автоматизированных библиотеках	Сообщения монтирования и сообщения об ошибках можно просматривать в автоматизированных библиотеках на клиентах командной строки администрирования в режиме монтирования или в режиме консоли. Сообщения монтирования посылаются в библиотеку, а не оператору. Сообщения о неполадках библиотеки отсылаются в очередь сообщений, связанных с монтированием.
Получение сведений о запросах к оператору, ожидающих выполнения	Для получения информации об отложенных требованиях для оператора введите команду QUERY REQUEST или просмотрите очередь сообщений монтирования на клиенте командной строки администрирования, запущенном в режиме монтирования. При использовании команды QUERY REQUEST сервер показывает запрашиваемые действия и время, оставшееся до истечения ожидания запрашиваемых действий.
Ответ на запросы к оператору	Когда сервер требует явного ответа на выполненный запрос монтирования, используйте команду REPLY. Параметр *номер_требования* задает идентификационный номер требования, указывающий серверу, какое из отложенных требований оператора выполнено. Этот трехзначный номер всегда появляется в сообщении с запросом.
Отмена требования для оператора	Чтобы отменить требование монтирования для библиотеки, введите команду CANCEL REQUEST. Для большинства запросов, связанных с автоматизированными библиотеками SCSI, оператор должен выполнить программное или аппаратное действие, чтобы отменить запрошенное монтирование. В случаях с такими запросами сервер не допускает использование команды CANCEL REQUEST. Команда CANCEL REQUEST должна содержать идентификационный номер запроса. Это номер указан в тексте запроса. Чтобы пометить запрашиваемый том как UNAVAILABLE, введите команду CANCEL REQUEST, задав параметр PERMANENT. Если задать параметр PERMANENT, то сервер не будет снова пытаться смонтировать запрошенный том. Например, это полезно, если том находится на удаленном сайте или недоступен по другой причине.

Задача	Подробности
Ответ на требование активации тома	Если серверу не удается обнаружить в автоматизированной библиотеке определенный том, который должен быть смонтирован, оператор получит запрос на регистрацию этого тома. Если запрашиваемый том доступен, поместите то его в библиотеку и активируйте. Дополнительную информацию смотрите в разделе Регистрация томов в автоматизированной библиотеке. Если затребованный том недоступен, измените режим доступа к тому, введя команду UPDATE VOLUME и задав параметр ACCESS=UNAVAILABLE. Затем отмените требование активации с помощью команды CANCEL REQUEST. Не отменяйте клиентский процесс, в результате которого был создан данный запрос. Используйте команду QUERY REQUEST для получения ID запроса, который вы хотите отменить. Если запрос сервера об активации тома не будет выполнен в течение периода ожидания монтирования для данного класса устройств в пуле хранения, то сервер пометит данный том как недоступный.
Как определить, какие тома смонтированы	Чтобы получить отчет о всех томах, которые в настоящий момент смонтированы для использования сервером, введите команду QUERY MOUNT. Этот отчет содержит сведения о том, какие тома смонтированы, какие накопители обращались к ним и какие тома используются.
Размонтирование бездействующих томов	Если том бездействует, то сервер оставляет его смонтированным в течение времени, заданного параметром задержки размонтирования для данного класса устройств. Использование задержки размонтирования позволяет сократить время доступа, если тома используются повторно. Чтобы размонтировать бездействующий том с диска, на котором он смонтирован, введите команду DISMOUNT VOLUME. Дополнительные сведения о настройке времени задержки размонтирования смотрите в разделе Управление интервалом времени, в течение которого том остается смонтированным.

Информация, связанная с данной:
QUERY REQUEST (Запросить информацию об одном или нескольких отложенных требованиях монтирования)

Управление ленточными накопителями

Вы можете запрашивать информацию о ленточных накопителях, обновлять их или удалять. Можно также очищать ленточные устройства и конфигурировать шифрование ленточного устройства и проверку правильности данных.

- Обновление накопителей
  Вы можете изменить атрибуты определения накопителя, чтобы перевести накопитель в отключенное состояние или деконфигурировать его.
- Проверка данных при операциях записи на ленту или чтения с ленты
  Для проверки данных и выявления поврежденных данных можно использовать функцию под названием 'защита логических блоков'. При использовании защиты логических блоков IBM Spectrum Protect вставляет значение проверки контрольной суммы в конце каждого логического блока данных, который записывается на ленту.
- Очистка ленточных накопителей
  Сервер можно использовать для управления очисткой ленточных накопителей. Сервер может управлять тем. как производится очистка ленточных накопителей в библиотеках SCSI.
- Замена ленточного накопителя
  Если заменяется накопитель в ленточной библиотеке, определенной для IBM Spectrum Protect, то необходимо удалить описания старого накопителя и пути к нему, а затем определить новый накопитель и путь.

Обновление накопителей

Вы можете изменить атрибуты определения накопителя, чтобы перевести накопитель в отключенное состояние или деконфигурировать его.

Об этой задаче

Можно изменить следующие атрибуты накопителя:

- Адрес элемента, если накопитель находится в SCSI
- Частота очистки
- Состояние накопителя: подключен или отключен

Ограничение: Если накопитель используется, вы не можете изменить ни номер элемента, ни имя устройства. Инструкции по отключению накопителей смотрите в разделе Отключение ленточных накопителей.
Если том смонтирован в накопителе, но он бездействует, его можно размонтировать явным образом. Инструкции по размонтированию бездействующего тома смотрите в разделе Управление серверными запросами на тома.

Процедура

- Измените адрес элемента накопителя, введя команду UPDATE DRIVE. Например, измените в библиотеке AUTO адрес элемента DRIVE3 на 119, введя следующую команду:

  ```
  update drive auto drive3 element=119
  ```

- Измените имя устройства для накопителя, введя команду UPDATE PATH. Например, чтобы изменить имя устройства накопителя с именем DRIVE3, введите следующую команду:  Операционные системы AIX

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
   device=/dev/rmt0
  ```

   Операционные системы Linux

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
   device=/dev/IBMtape0
  ```

   Операционные системы Windows

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
     device=mt3.0.0.0
  ```

- Отключение ленточных накопителей
  Ленточный накопитель можно отключить в процессе его использования. Например, можно отключить накопитель для обслуживания.

Ссылки, связанные с данной:
UPDATE PATH (изменение пути)
Информация, связанная с данной:
UPDATE DRIVE (обновление накопителя)

Проверка данных при операциях записи на ленту или чтения с ленты

Для проверки данных и выявления поврежденных данных можно использовать функцию под названием 'защита логических блоков'. При использовании защиты логических блоков IBM Spectrum Protect вставляет значение проверки контрольной суммы в конце каждого логического блока данных, который записывается на ленту.

С помощью защиты логических блоков можно обнаруживать ошибки, происходящие при записи данных на ленту и при передаче данных с ленточного устройства в IBM Spectrum Protect через сеть хранения данных. Устройства, поддерживающие защиту логических блоков, проверяют данные во время операций чтения и записи. Сервер IBM Spectrum Protect проверяет данные во время операций чтения.

Если проверка на устройстве завершается с ошибкой во время операций записи, это может означать, что данные повреждены при передаче на ленту. В таком случае сервер IBM Spectrum Protect завершает операцию записи с ошибкой. Необходимо перезапустить операцию, чтобы продолжить работу. Если проверка на устройстве выдает ошибку во время операции чтения, это может означать, что ленточный носитель поврежден. Если проверка на сервере IBM Spectrum Protect выдает ошибку во время операции чтения, это может означать, что данные повреждены при передаче с ленточного устройства; сервер попытается выполнить операцию еще раз. Если проверка постоянно завершается с

ошибкой, сервер IBM Spectrum Protect создает сообщение об ошибке, которое означает проблему оборудования или подключения.

Если защита логических блоков отключена на ленточном устройстве или это устройство не поддерживает защиту логических блоков, сервер IBM Spectrum Protect может прочитать защищенные данные. Однако эти данные не проверяются.

Защита логических данных лучше защиты контрольной суммы, которую можно задать при определении или обновлении пула хранения. Если вы зададите проверку CRC для пула хранения, то данные будут проверяться только в ходе операций по аудиту томов. Ошибки выявляются после записи данных на ленту.

Ограничения:

- Нельзя использовать защиту логических блоков для последовательных данных, таких как наборы резервных копий и резервные копии базы данных.
- Проверка CRC отрицательно влияет на производительность, так как и на клиенте, и на сервере для вычисления и сравнения значений CRC потребуется использовать больше процессорных ресурсов.
- В случае чистого тома, если вы зададите защиту логического блока для операций чтения-записи (LBPROTECT=READWRITE), никогда не изменяйте значение параметра после записи данных на том. Изменение значения параметра в течение срока жизни тома на сервере IBM Spectrum Protect не поддерживается.

- Накопители, поддерживающие защиту логических блоков
  Защита логических блоков доступна только для устройств типов 3592, LTO и ECARTRIDGE. К накопителям, поддерживающим 3592, относятся IBM TS1130, TS1140 и более новые поколения. К возможным накопителям LTO относятся накопители IBM LTO-5 и поддерживаемые накопители LTO-6. В число поддерживаемых накопителей Oracle StorageTek входят накопители с форматом T10000C и T10000D.
- Включение и отключение защиты логических блоков
  Вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи. Также можно выключить защиту логических блоков. По умолчанию защита логических блоков отключена, так как проверка контрольной суммы (cyclic redundancy check, CRC) на сервере и на ленточном устройстве влияет на производительность.
- Операции чтения/записи для томов с защитой логических блоков
  Операции чтения/записи для освобождения или заполнения томов зависят от наличия в томе защиты логических блоков. Защищенные и незащищенные блоки нельзя смешивать в одном томе.
- Управление пулами хранения в ленточной библиотеке
  Чтобы хранить в одной библиотеке и защищенные, и незащищенные данные, надо создать различные классы устройств и различные пулы хранения для разделения этих данных. Если класс устройства связан с защищенными данными, вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи.

Накопители, поддерживающие защиту логических блоков

Защита логических блоков доступна только для устройств типов 3592, LTO и ECARTRIDGE. К накопителям, поддерживающим 3592, относятся IBM TS1130, TS1140 и более новые поколения. К возможным накопителям LTO относятся накопители IBM LTO-5 и поддерживаемые накопители LTO-6. В число поддерживаемых накопителей Oracle StorageTek входят накопители с форматом T10000C и T10000D.

В следующей таблице показаны носители и форматы, которые можно использовать с накопителями, поддерживающими защиту логических блоков.

Накопитель	Ленточный носитель	Форматы накопителей
IBM TS1130	3592 Generation 2	3592-3 и 3592-3C
IBM TS1140	3592 Generation 2 3592 поколения 3	Поколение 2: 3592-3 и 3592-3C Поколение 3: 3592-4 и 3592-4C
IBM TS1150	3592 поколения 3 3592, поколение 4	Поколение 4: 3592-5 и 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 и Ultrium 5C

Накопитель	Ленточный носитель	Форматы накопителей
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 и Ultrium 6C Ultrium 5 и Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 и Ultrium 7C Ultrium 6 и Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C и T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D и T10000D-C

Советы:

- Чтобы включить логическую защиту блока для ленточного тома и затем снова использовать том для поддержки данных, надо включить логическую защиту блока для класса устройства и диска.
- Если у вас есть накопитель 3592, LTO или Oracle StorageTek, не поддерживающий защиту логических блоков, его программно-аппаратное обеспечение можно обновить до версии, поддерживающей защиту логических блоков.

Доступна защита логических блоков для накопителей в библиотеках SCSI . Самую свежую информацию о поддержке защиты логических блоков смотрите в техническом замечании 1568108.

Чтобы можно было использовать защиту логических блоков для операций записи, все накопители в библиотеке должны поддерживать защиту логических блоков. Если накопитель не поддерживает защиту логических блоков, тома, доступные для чтения и записи, монтироваться не будут. Однако сервер может использовать такой накопитель для монтирования томов, доступных только для чтения. Защищенные данные читаются и проверяться сервером IBM Spectrum Protect, если включена поддержка защиты логических блоков для операций чтения/записи.

Включение и отключение защиты логических блоков

Вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи. Также можно выключить защиту логических блоков. По умолчанию защита логических блоков отключена, так как проверка контрольной суммы (cyclic redundancy check, CRC) на сервере и на ленточном устройстве влияет на производительность.

Об этой задаче

Операции чтения/записи для освобождения или заполнения томов зависят от наличия в томе защиты логических блоков. Защищенные и незащищенные блоки нельзя смешивать в одном томе. Если изменить параметр защиты логических блоков, это изменение будет применено только к пустым томам. Заполняемые и полные тома поддерживают свое состояние защиты логических блоков, пока они не будут пустыми и готовыми для нового заполнения. Например, если сервер выберет том, связанный с классом устройств с защитой логических блоков, сервер продолжит запись защищенных данных на этот том.
Ограничение: Защита логических блоков доступна только для некоторых типов устройств. Дополнительную информацию смотрите в разделе Накопители, поддерживающие защиту логических блоков.

Процедура

1. Чтобы включить защиту логических блоков для типов устройств 3592, LTO и ECARTRIDGE, введите команду DEFINE DEVCLASS или UPDATE DEVCLASS и задайте параметр LBPROTECT. Например, чтобы задать защиту логических блоков во время операций чтения и записи для класса устройств 3592 с именем 3592_lbprotect, введите следующую команду:

   ```
   define devclass 3592_lbprotect library=3594 lbprotect=readwrite
   ```

   Советы:
   - Если изменить значение параметра LBPROTECT с NO на READWRITE или WRITEONLY и сервер выберет заполняющийся том без защиты логических блоков, он будет выдавать сообщение при всяком монтировании тома. Это сообщение информирует, что данные будут записаны в том без защиты логических блоков. Чтобы предотвратить появление этого сообщения или чтобы IBM Spectrum Protect выполнял запись данных только с защитой логических блоков, сделайте заполняющиеся тома без защиты логических блоков доступными только для чтения.
   - Чтобы повысить производительность, не указывайте параметр CRCDATA в команде DEFINE STGPOOL или UPDATE STGPOOL.

- Когда данные проверяются во время операций чтения как на накопителе, так и на сервере IBM Spectrum Protect, это может привести к снижению производительности сервера во время операций восстановления и извлечения. Чтобы сократить время, которое требуется для выполнения операций по восстановлению и извлечению данных, измените значение параметра LBPROTECT с READWRITE на WRITEONLY. После восстановления или извлечения данных можно снова изменить значение параметра LBPROTECT на READWRITE.

2. Чтобы выключить защиту логических блоков, введите команду DEFINE DEVCLASS или UPDATE DEVCLASS и задайте параметр LBPROTECT=NO.
   Ограничение: Если защита логических блоков отключена, сервер не выполняет запись на пустую ленту с защитой логических блоков. Однако если выбран заполняющийся том с защитой логических блоков, сервер продолжит запись в том с защитой логических блоков. Чтобы сервер не выполнял запись на ленту с защитой логических блоков, сделайте заполняющиеся тома с защитой логических блоков доступными только для чтения. При чтении данных результаты CRC (контрольной суммы) не проверяются ни на накопителе, ни на сервере.

   Если произойдет авария и на площадке восстановления после аварии не окажется накопителей, поддерживающих защиту логических блоков, нужно задать параметр LBPROTECT=NO. Если для записи используются ленточные накопители, то нужно заменить доступ к томам с защищенными данными на "только для чтения", чтобы сервер не использовал эти тома.

   Если сервер должен включить защиту логических блоков, сервер выдает сообщение об ошибке, которое указывает, что накопитель не поддерживает защиту логических блоков.

Дальнейшие действия

Для определения, есть ли у тома защита логических блоков, введите команду QUERY VOLUME и проверьте значение в поле `Защита логических блоков`.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
UPDATE STGPOOL (обновить пул хранения)
Информация, связанная с данной:
DEFINE STGPOOL (определение тома в пуле хранения)
QUERY VOLUME (Запросить информацию о томах пула хранения)
UPDATE DEVCLASS (изменение класса устройства)

Операции чтения/записи для томов с защитой логических блоков

Операции чтения/записи для освобождения или заполнения томов зависят от наличия в томе защиты логических блоков. Защищенные и незащищенные блоки нельзя смешивать в одном томе.

Если для изменения параметра защиты логических блоков используется команда UPDATE DEVCLASS, это изменение применяется только к пустым томам. Заполняемые и полные тома поддерживают свое состояние защиты логических блоков, пока они не будут пустыми и готовыми для нового заполнения.

Предположим, например, что вы измените значение параметра LBPROTECT с READWRITE на NO. Если сервер выберет том, который связан с классом устройства и на котором задана защита логических блоков, сервер по-прежнему будет записывать на том защищенные данные.

Советы:

- Если накопитель не поддерживает защиту логических блоков, смонтировать тома с защитой логических блоков для операций записи не удастся. Чтобы предотвратить монтирование сервером защищенных томов для операций записи, измените доступ к тому на предназначенный только для чтения. Отключите также защиту логических блоков, чтобы предотвратить включение сервером этой возможности для ленточных накопителей.
- Если диск не поддерживает защиту логических блоков и такая защита отключена, сервер читает данные с защищенных томов. Однако эти данные не проверяются сервером и ленточным накопителем.

Информация, связанная с данной:
QUERY VOLUME (Запросить информацию о томах пула хранения)
UPDATE DEVCLASS (изменение класса устройства)

Управление пулами хранения в ленточной библиотеке

Чтобы хранить в одной библиотеке и защищенные, и незащищенные данные, надо создать различные классы устройств и различные пулы хранения для разделения этих данных. Если класс устройства связан с защищенными данными, вы можете определить защиту логических блоков для операций чтения и записи или только для операций записи.

Чтобы задать классы устройства и пулы хранения для библиотеки TS3500 с накопителями LTO-5 для защищенных и незащищенных данных, можно ввести ряд команд, как показано в следующем примере:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

Ссылки, связанные с данной:

DEFINE DEVCLASS (Задать класс устройств)

Информация, связанная с данной:

DEFINE LIBRARY (Задать библиотеку)

DEFINE STGPOOL (определение тома в пуле хранения)

Очистка ленточных накопителей

Сервер можно использовать для управления очисткой ленточных накопителей. Сервер может управлять тем. как производится очистка ленточных накопителей в библиотеках SCSI.

Об этой задаче

Для очистки ленточных накопителей необходимы системные полномочия или неограниченные полномочия на хранение. В случае автоматизированных библиотек можно автоматизировать очистку, задав частоту операций очистки и зарегистрировав чистящий картридж в перечне томов библиотеки. IBM Spectrum Protect смонтирует чистящий картридж в соответствии с заданными значениями. Особые замечания касаются случая, когда планируется использовать очистку накопителей под управлением сервера в библиотеке SCSI, которая поддерживает автоматическую очистку накопителей на аппаратном уровне.

Совет: Если автоматизированная ленточная библиотека поддерживает очистку накопителей в библиотеке, убедитесь, что эта функция включена.

Вы можете предотвратить преждевременное изнашивание головок для чтения и записи накопителей, используя функции очистки библиотеки, которые предоставляет ваш производитель устройств.

Накопители и библиотеки от разных производителей различаются тем, как они управляют чистящими картриджами и как они сообщают о присутствии чистящего картриджа в накопителе. Драйвер устройства может не открыть накопитель, в котором содержится чистящий картридж. Коды считывания и коды ошибок, выдаваемые устройствами для чистки накопителя, отличаются. Очистка накопителей библиотеки обычно неизвестна приложениям. В связи с этим IBM Spectrum Protect не всегда обнаруживает чистящие картриджи в накопителях и может не определить время начала чистки.

Некоторые устройства требуют небольшой период простоя между запросами на монтирование для запуска чистки накопителя. Однако IBM Spectrum Protect пытается свести к минимуму время простоя накопителя. Результатом может быть неэффективное выполнение чистки накопителя библиотеки. Если это происходит, используйте IBM Spectrum Protect для управления очисткой накопителей. Можно задать частоту очистки в соответствии с рекомендациями производителя.

- Методы очистки ленточных накопителей
  Со временем читающие головки ленточных накопителей могут загрязниться, что может вызвать ошибки чтения и записи. Чтобы предотвратить эти проблемы, включите очистку магнитных лент. Очистку лент можно включить с накопителя или из IBM Spectrum Protect.
- Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке
  При конфигурировании очистки накопителей в автоматизированной библиотеке под управлением сервера вы можете указать, как часто должна производиться чистка накопителей.
- Устранение ошибок, связанных с очисткой накопителей
  При перемещении картриджей в библиотеке вы можете поместить картридж с данными туда, где должен находиться чистящий картридж. Ознакомьтесь с процессом, который выполнит сервер, и генерируемыми сообщениями, чтобы вы смогли устранить проблему.

Методы очистки ленточных накопителей

Со временем читающие головки ленточных накопителей могут загрязниться, что может вызвать ошибки чтения и записи. Чтобы предотвратить эти проблемы, включите очистку магнитных лент. Очистку лент можно включить с накопителя или из IBM Spectrum Protect.

Можно выбрать использование способа очистки библиотечного накопителя или способ очистки накопителя IBM Spectrum Protect, но не оба способа одновременно. Некоторые библиотеки SCSI обеспечивают возможность автоматической очистки накопителей. Выберите метод очистки библиотечных накопителей, если он доступен. Если он недоступен или вызывает проблемы, используйте IBM Spectrum Protect для управления очисткой библиотечных накопителей.

Метод очистки библиотечных накопителей

У способа очистки библиотечных накопителей есть несколько преимуществ для автоматических ленточных библиотек, использующих эту функцию:

- Понижается нагрузка на администратора IBM Spectrum Protect по физическому управлению очисткой картриджей.
- Снижается интенсивность использования картриджей очистки. Большинство библиотек отслеживает, сколько раз можно очищать ленты, на основании индикаторов аппаратных компонентов. IBM Spectrum Protect использует необработанное число.
- Уменьшает число необязательных очисток. В современных ленточных носителях не требуются очистки через фиксированные интервалы времени, так как они могут определить, когда нужна очистка, и затребовать ее.

Производители, которые предоставляют метод очистки библиотечных накопителей, рекомендуют его использовать, чтобы предотвратить преждевременный износ головок чтения/записи в накопителях. Накопители и библиотеки от разных производителей различаются тем, как они управляют чистящими картриджами и как они сообщают о присутствии чистящего картриджа в накопителе. Драйвер устройства может не открыть накопитель, в котором содержится чистящий картридж. Коды считывания и коды ошибок, выдаваемые устройствами для чистки накопителя, отличаются. Чистка накопителя библиотеки обычно скрыта от программ. Однако IBM Spectrum Protect не всегда обнаруживает чистящие картриджи в накопителях и может не определить время начала чистки.

Способы очистки накопителей IBM Spectrum Protect

Некоторые устройства требуют небольшой период простоя между запросами на монтирование для запуска чистки накопителя. Однако IBM Spectrum Protect пытается свести к минимуму время простоя накопителя. Результатом может быть неэффективное выполнение чистки накопителя библиотеки. Если это происходит, попробуйте использовать IBM Spectrum Protect для управления чисткой накопителей. Установите частоту очистки, соответствующую рекомендациям производителя.

Если IBM Spectrum Protect управляет процессом очистки накопителей, отключите функцию очистки библиотечных накопителей, чтобы избежать проблем. Если включена функция очистки библиотечных носителей, некоторые устройства автоматически перемещают чистящий картридж, обнаруженный в библиотеке, в выделенные для него слоты библиотеки. Невозможно зарегистрировать чистящий картридж в перечне библиотеки IBM Spectrum Protect, пока не отключена собственная функция очистки библиотечных носителей.

Чтобы включить очистку с накопителя, следуйте инструкциям, которые предоставляет производитель накопителя. Чтобы узнать, как включить очистку с использованием IBM Spectrum Protect, смотрите раздел Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке.

Конфигурирование сервера для очистки накопителей в автоматизированной библиотеке

При конфигурировании очистки накопителей в автоматизированной библиотеке под управлением сервера вы можете указать, как часто должна производиться чистка накопителей.

Прежде чем начать

Определите, как часто следует производить очистку накопителя. Этот шаг необходим, чтобы вы смогли задать соответствующее значение для параметра CLEANFREQuency в команде DEFINE DRIVE или UPDATE DRIVE. Например, чтобы производить очистку накопителя после обработки 100 ГБ данных на накопителе, задайте параметр CLEANFREQUENCY=100.

Рекомендации по частоте очистки смотрите в документации производителя накопителей. Если в документации представлены рекомендации по частоте очистки, исходя из часов использования, преобразуйте значение в гигабайты, выполнив следующие шаги:

1. На основе значения 'байт в секунду' для накопителя определите значение в гигабайтах в час.
2. Умножьте значение в гигабайтах в час на рекомендуемое количество часов использования между чистками.
3. Результатом этого действия и будет частота очистки.

Можно задать либо значение параметра CLEANFREQUENCY, либо можно указать ASNEEDED, чтобы производить очистку накопителя, когда это потребуется.
Ограничения:

1. Для накопителей IBM® 3592 нужно задавать числовое значение параметра CLEANFREQUENCY. Если использовать частоту очистки, указанную в документации по продукту, вы не произведете очистку накопителей сверх необходимого.
2. Значение параметра CLEANFREQUENCY=ASNEEDED работает не для всех ленточных накопителей. Чтобы узнать, поддерживает ли накопитель данную функцию, смотрите информацию для вашей операционной системы:
   - Операционные системы AIXОперационные системы WindowsПоддерживаемые устройства для AIX и Windows
   - Операционные системы LinuxПоддерживаемые устройства для Linux

   В техническом замечании щелкните по имени накопителя, чтобы увидеть подробную информацию. Если значение ASNEEDED не поддерживается, задайте число гигабайт.

Процедура

Чтобы сконфигурировать управляемую сервером очистку накопителя в автоматизированной библиотеке, выполните следующие шаги:

Определите или измените накопители в библиотеке, используя параметр CLEANFREQUENCY в командах DEFINE DRIVE или UPDATE DRIVE. Например, чтобы производить очистку накопителя DRIVE1 после обработки 100 ГБ данных, введите следующую команду:

```
update drive autolib1 drive1 cleanfrequency=100
```

Результаты

После того как чистящий картридж будет зарегистрирован, сервер будет монтировать его в накопитель, когда понадобится произвести очистку. Сервер будет использовать чистящий картридж для указанного числа очисток. Дополнительную информацию смотрите в разделе Операции с чистящими картриджами.

Дальнейшие действия

Активируйте чистящий картридж в перечне томов библиотеки, следуя инструкциям в разделе Активация чистящего картриджа в библиотеке.

- Активация чистящего картриджа в библиотеке
  Чтобы включить автоматическую очистку ленточных накопителей, нужно активировать чистящий картридж в перечне томов автоматизированной библиотеки.
- Операции с чистящими картриджами
  Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Информация, связанная с данной:
DEFINE DRIVE (Задать накопитель для библиотеки)
UPDATE DRIVE (обновление накопителя)

Активация чистящего картриджа в библиотеке

Чтобы включить автоматическую очистку ленточных накопителей, нужно активировать чистящий картридж в перечне томов автоматизированной библиотеки.

Об этой задаче

При активации чистящего картриджа в библиотеке убедитесь, что он правильно идентифицирован сервером как чистящий картридж. Убедитесь, что чистящий картридж не находится в слоте, который обнаружен процессом поиска. Из-за неправильно расположенного чистящего картриджа могут возникать ошибки и задержки до 15 минут и более.

Предпочтительный метод заключается в активации чистящих картриджей по отдельности. Если вам нужно активировать как картриджи с данными, так и чистящие картриджи, сначала поместите картриджи с данными в библиотеку и активируйте их. Затем отдельно активируйте чистящий картридж в библиотеке.

Процедура

Чтобы активировать чистящий картридж в библиотеке, введите команду CHECKIN LIBVOLUME. Например, чтобы активировать чистящий картридж с именем AUTOLIB1, введите следующую команду:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10
 checklabel=no
```

Сервер попросит поместить картридж в порт входа/выхода или в конкретный слот.

Ссылки, связанные с данной:
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)

Операции с чистящими картриджами

Чтобы убедиться, что ленточные накопители подвергаются очистке, когда это необходимо, и чтобы избежать проблем с пространством хранения на ленте, следуйте рекомендациям.

Мониторинг процесса очистки
: Если в библиотеке активируется чистящий картридж и нужно очистить накопитель, сервер размонтирует том данных и запустит операцию очистки. Если операция очистки завершится неудачно или будет отменена либо если чистящего картриджа нет, вы можете не узнать, что требуется очистка накопителя. Из-за этой проблемы необходимо следить за сообщениями об очистке, чтобы обеспечить своевременную очистку накопителей. При необходимости введите команду CLEAN DRIVE, чтобы сервер попытался еще раз произвести очистку, или вручную загрузите чистящий картридж в накопитель.

Использование нескольких чистящих картриджей
: Сервер будет использовать чистящий картридж для числа очисток, указанного при регистрации чистящего картриджа. Если зарегистрировать два или несколько чистящих картриджей, сервер будет использовать только один из них, пока не будет достигнуто заданное для картриджа число очисток. Затем сервер использует следующий чистящий картридж. Если зарегистрировать два или несколько чистящих картриджей и ввести две или несколько команд CLEAN DRIVE одновременно, сервер будет использовать несколько картриджей одновременно и зарегистрирует оставшееся количество очисток для каждого картриджа.

Ссылки, связанные с данной:
AUDIT LIBRARY (аудит томов автоматизированной библиотеки)
CHECKIN LIBVOLUME (регистрация тома хранения в библиотеке)
CLEAN DRIVE (очистка накопителя)
LABEL LIBVOLUME (запись метки на том библиотеки)
Информация, связанная с данной:
QUERY LIBVOLUME (Запросить информацию о томе библиотеки)

Устранение ошибок, связанных с очисткой накопителей

При перемещении картриджей в библиотеке вы можете поместить картридж с данными туда, где должен находиться чистящий картридж. Ознакомьтесь с процессом, который выполнит сервер, и генерируемыми сообщениями, чтобы вы смогли устранить проблему.

Когда требуется очистить накопитель, сервер загружает в него картридж, который, согласно его базе данных, должен быть чистящим. Затем накопитель переходит в состояние READY и IBM Spectrum Protect определяет, что картридж является картриджем данных. Сервер выполняет следующие действия:

1. Сервер пытается считать внутреннюю метку ленты из картриджа данных.

2. Сервер извлекает картридж из накопителя и перемещает его в обратно в слот для чистящего картриджа в пределах библиотеки. Если извлечение не удается, то сервер помечает накопитель как отключенный и выдает сообщение, что картридж все еще находится в накопителе.
3. Сервер резервирует чистящий картридж, чтобы предотвратить его повторный выбор для следующего запроса очистки накопителя. Чистящий картридж остается в библиотеке, но больше не фигурирует в перечне библиотеки IBM Spectrum Protect.
4. Сервер сравнивает имя тома с текущим перечнем библиотеки, томами пула хранения и файлом хронологии томов, используя внутреннюю метку ленты.
    - Если имя тома не найдено в перечне библиотеки, возможно, картридж с данными был по ошибке активирован как чистящий картридж. При отмене активации тома никаких дальнейших действий от вас не требуется.
    - Если имя тома найдено в перечне библиотеки, сервер сгенерирует сообщение о том, что требуется вмешательство оператора и аудит библиотеки. Чтобы устранить проблему, выполните инструкции из раздела Аудит перечня томов в библиотеке.

Замена ленточного накопителя

Если заменяется накопитель в ленточной библиотеке, определенной для IBM Spectrum Protect, то необходимо удалить описания старого накопителя и пути к нему, а затем определить новый накопитель и путь.

Замена определений накопителей и путей необходима, даже если используется новый накопитель того же типа, тот же логический адрес, физический адрес, идентификатор SCSI и номер порта. Алиасы устройств могут меняться при изменении подключений накопителей.

Если новый накопитель поддерживает новый формат носителей, то может возникнуть необходимость описать новую логическую библиотеку, класс устройства и пул хранения. Процедуры настройки политики для нового накопителя в библиотеке с несколькими накопителями зависят от типов накопителей и носителей в библиотеке.

- Удаление ленточных накопителей
  Из библиотеки можно удалять ленточные накопители. Например, можно удалить накопитель, который вы больше не используете, или накопитель, который вы хотите заменить.
- Замена накопителей другими накопителями того же типа
  Чтобы добавить накопитель, поддерживающий тот же формат носителей, что и заменяемый им накопитель, нужно задать новое устройство и путь.
- Перенос данных на обновленные накопители
  Если вы обновляете все ленточные накопители в библиотеке, вы можете сохранить существующие определения правил политики, чтобы производить перенос и удаление устаревших существующих данных, и сможете использовать новые накопители для сохранения данных.

Удаление ленточных накопителей

Из библиотеки можно удалять ленточные накопители. Например, можно удалить накопитель, который вы больше не используете, или накопитель, который вы хотите заменить.

Процедура

1. Завершите работу сервера IBM Spectrum Protect и операционной системы.
2. Удалите старый накопитель и, следуя инструкциям производителя, установите новый накопитель.
3. Перезапустите операционную систему и сервер IBM Spectrum Protect.
4. Удалите путь от сервера к накопителю. Например, чтобы удалить путь от SERVER1 до LIB1, введите следующую команду:

   ```
   delete path server1 lib1 srctype=server desttype=drive
   ```

5. Удалите описание накопителя. Например, введите следующую команду, чтобы удалить накопитель с именем DLT1 из библиотечного устройства с именем LIB1:

   ```
   delete drive lib1 dlt1
   ```

Ссылки, связанные с данной:
DELETE DRIVE (Удалить накопители из библиотеки)
DELETE PATH (удаление пути)

Замена накопителей другими накопителями того же типа

Чтобы добавить накопитель, поддерживающий тот же формат носителей, что и заменяемый им накопитель, нужно задать новое устройство и путь.

Об этой задаче

Если в библиотеке есть только одна модель накопителя и вы хотите заменить накопитель, вы должны заменить накопитель накопителем той же модели. Если в библиотеке есть комбинация моделей накопителей и вы хотите заменить накопитель, вы должны заменить накопитель накопителем любой модели, которая существует в библиотеке.

Процедура

1. Удалите определения пути и накопителя для старого накопителя. Например, чтобы удалить накопитель с именем DRIVE1 из библиотеки LIB1, введите следующую команду:

   ```
   delete path server2 drive1 srctype=server desttype=drive library=lib1
   delete drive lib1 drive1
   ```

2. Выключите библиотеку, размонтируйте исходный накопитель, замените его новым накопителем и включите библиотеку.
3. Обновите хост-систему, чтобы убедиться, что система обнаружила новый накопитель.
4. Опишите новый накопитель и путь. Например, чтобы задать новый накопитель, DRIVE2, и путь к нему с сервера SERVER2, если вы используете драйвер устройств IBM Spectrum Protect, введите следующие команды:

    Операционные системы AIX

   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=/dev/mt0
   ```

    Операционные системы Linux

   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=/dev/tsmscsi/mt0
   ```

    Операционные системы Windows

   ```
   define drive lib1 drive2
   define path server2 drive2 srctype=server desttype=drive library=lib1
      device=mt3.0.0.1
   ```

   Совет: Можно использовать существующие описания библиотек, классов устройства и пулов хранения.

Ссылки, связанные с данной:
DELETE DRIVE (Удалить накопители из библиотеки)
DELETE PATH (удаление пути)

Перенос данных на обновленные накопители

Если вы обновляете все ленточные накопители в библиотеке, вы можете сохранить существующие определения правил политики, чтобы производить перенос и удаление устаревших существующих данных, и сможете использовать новые накопители для сохранения данных.

Прежде чем начать

В следующем сценарии предполагается, что у вас уже есть первичный пул хранения для класса устройств DISK с именем POOL1.

Процедура

1. Чтобы перенести данные в пул хранения, созданный для новых накопителей, задайте параметр NEXTSTGPOOL. Например, чтобы перенести данные из существующего пула хранения POOL1 в новый пул хранения, POOL2,

введите следующую команду:

```
update stgpool pool1 nextstgpool=pool2
```

2. Измените определения классов управления, чтобы сохранить данные в новом пуле хранения DISK, при помощи команды UPDATE MGMTCLASS.

Ссылки, связанные с данной:
UPDATE MGMTCLASS (обновление класса управления)
UPDATE STGPOOL (обновить пул хранения)
Информация, связанная с данной:
DEFINE STGPOOL (определение тома в пуле хранения)

Защита сервера IBM Spectrum Protect

Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.

- Управление администраторами
  Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.
- Изменение требований к паролям
  Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.
- Защита сервера в системе
  Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Процедура

Чтобы изменить параметры администратора, выполните описанные ниже шаги.

Задача	Процедура

Добавить администратора	Чтобы добавить администратора, ADMIN1, с системными полномочиями и задать пароль, выполните следующие шаги:
	a. Зарегистрируйте администратора и задайте Pa$#$twO в качестве пароля, введя следующую команду:
	`register admin admin1 Pa$#$twO`
	b. Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`

Задача	Процедура

Изменить административные полномочия	Измените уровень полномочий для администратора ADMIN1.
	• Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`
	• Аннулируйте системные полномочия администратора, введя следующую команду:
	`revoke authority admin1 classes=system`

Удалить администраторов	Аннулируйте для администратора ADMIN1 доступ к серверу IBM Spectrum Protect, введя следующую команду: `remove admin admin1`
Временно запретите доступ к серверу	Заблокируйте или разблокируйте администратора, введя команду LOCK ADMIN или UNLOCK ADMIN.

Понятия, связанные с данным:
Планирование ролей администратора

Изменение требований к паролям

Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.

Об этой задаче

Применяя аутентификацию на основе паролей и управляя ограничениями паролей, вы защищаете данные и серверы от потенциальных угроз безопасности.

Процедура

Чтобы изменить требования к паролям для серверов IBM Spectrum Protect, выполните описанные ниже задачи.

Табл. 1. Задачи по аутентификации для серверов IBM Spectrum Protect

Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число неудачных попыток в поле Предел неудачных попыток входа в систему. Значение по умолчанию при установке равно 0.
Задайте минимальную длину пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число символов в поле Минимальная длина пароля.

Задача	Процедура
Задайте срок действия паролей.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте срок в днях в поле Общий срок действия паролей.
Отключите аутентификацию на основе паролей.	По умолчанию сервер автоматически использует аутентификацию с помощью пароля. При аутентификации пароля все пользователи для получения доступа к серверу должны вводить пароль. Запретить аутентификацию пароля можно только для паролей, аутентификация которых выполняется на сервере (LOCAL). Отключая аутентификацию на основе паролей, вы делаете сервер доступным для угроз безопасности.

Задать метод аутентификации по умолчанию.	Введите команду SET DEFAULTAUTHENTICATION. Например, чтобы использовать сервер как метод аутентификации по умолчанию, введите следующую команду:
	
	`set defaultauthentication local`
	
	Чтобы обновить клиентский узел для аутентификации на сервере, включите `AUTHENTICATION=LOCAL` в команду UPDATE NODE:
	
	`update node authentication=local`

Защита сервера в системе

Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Процедура

Убедитесь, что неавторизованные пользователи не могут получить доступ к каталогам для базы данных сервера и экземпляра сервера. Оставьте для этих каталогов параметры доступа, которые вы сконфигурировали во время реализации.

- Ограничение доступа пользователей к серверу
  Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Остановка и запуск сервера

Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.

Прежде чем начать

Чтобы остановить и запустить сервер IBM Spectrum Protect, требуются системные полномочия или полномочия оператора.

- Остановка сервера
  Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию

базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

- Запуск сервера для задач обслуживания или реконфигурирования
  Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Остановка сервера

Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

Об этой задаче

При вводе команды HALT для остановки сервера происходят следующие действия:

- Все процессы и сеансы узлов клиентов будут отменены.
- Все текущие транзакции будут остановлены. (При перезапуске сервера будет произведен откат транзакций.)

Процедура

Чтобы подготовить систему и остановить сервер, выполните следующие шаги:

1. Запретите запуск новых сеансов клиентских узлов, введя команду DISABLE SESSIONS:

   ```
   disable sessions all
   ```

2. Определите, не выполняются ли какие-либо сеансы клиентских узлов или процессы, выполнив следующее:
   a. На странице Центра операций Обзор посмотрите в области Активность общее число процессов и сеансов, которые активны в настоящий момент. Если это число заметно отличается от значения, которое обычно показано во время повседневного управления хранением, то просмотрите другие индикаторы состояния в Центре операций, чтобы определить, ошибка ли это.
   b. Смотрите график в области Активность, чтобы сравнить объем сетевого трафика за следующие периоды:
      - Текущий период, то есть, самые последние 24 часа
      - Предыдущий период, то есть, за 24 часа до текущего периода

      Если на графике за предыдущий период показано ожидаемый объем трафика, существенные различия с графиком за текущий период могут указывать на проблему.
   c. Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения. Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, получите информацию о процессах при помощи команд администрирования. Введите команду QUERY PROCESS для запроса процессов и получения информации о сеансах при помощи команды QUERY SESSION.
3. Дождитесь завершения сеансов клиентских узлов или отмените их. Чтобы отменить процессы и сеансы, сделайте следующее:
   - Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   - Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   - Нажмите кнопку Отмена.
   - Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, отмените сеансы при помощи команд администрирования. Введите команду CANCEL SESSION, чтобы отменить сеанс и процессы при помощи команды CANCEL PROCESS.
     Совет: Если процесс, который вы хотите отменить, ожидает монтирования ленточного тома, требование монтирования будет отменено. Например, если вы введете команду EXPORT, IMPORT или MOVE DATA, команда может инициировать процесс, для которого потребуется смонтировать ленточный том. Однако, если ленточный том монтируется автоматизированной библиотекой, операция отмены может не иметь силы, пока не завершится процесс монтирования. В зависимости от вашей системной среды на это может потребоваться несколько минут.
4. Остановите сервер с помощью команды HALT:

   ```
   halt
   ```

Запуск сервера для задач обслуживания или реконфигурирования

Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

   ```
   halt
   ```

2. Запустите сервер, используя метод, который вы используете в производственном режиме. Выполните инструкции для вашей операционной системы.
   -  Операционные системы AIXЗапуск экземпляра сервера
   -  Операционные системы LinuxЗапуск экземпляра сервера
   - Операционные системы WindowsЗапуск экземпляра сервера

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Планирование обновления сервера

Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.

Об этой задаче

Выполните следующие рекомендации:

- Предпочтительный метод - обновить сервер с использованием мастера установки. Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.

- Если доступны обновления и для серверного компонента, и для компонента Центр операций, выберите переключатели, указывающие, что нужно обновить оба компонента.

Процедура

1. Проверьте список пакетов исправлений и промежуточных исправлений. Смотрите раздел Техническое замечание 1239415.
2. Ознакомьтесь с усовершенствованиями продукта, описанными в файлах readme.
   Совет: Получив пакет установки со страницы сайт поддержки IBM Spectrum Protect, вы также сможете получить доступ к файлу readme.
3. Убедитесь что версия, до которой вы обновляете сервер, совместима с другими компонентами, например, с агентами хранения и клиентами библиотек. Смотрите раздел Техническое замечание 1302789.
4. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены. Смотрите раздел Техническое замечание 1053218.
5. Прочтите инструкции по обновлению. Обязательно создайте резервную копию базы данных сервера, информации о конфигурации устройств и файла хронологии томов.

Дальнейшие действия

Чтобы установить пакет исправлений или промежуточное исправление, следуйте инструкциям для вашей операционной системы:

- Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect

Информация, связанная с данной:
Процесс обновления и перенастройки - Часто задаваемые вопросы

Подготовка к отключению или обновлению системы

Подготовьте IBM Spectrum Protect, чтобы при плановом отключении питания или обновлении системы сохранять вашу систему в непротиворечивом состоянии.

Об этой задаче

Убедитесь, что вы запланировали регулярные действия по управлению, защите и обслуживанию сервера. Информацию о таких операциях планирования, как резервное копирование базы данных, резервное копирование файлов конфигурации устройств и резервное копирование хронологии томов, смотрите в разделе Как задать расписания для операций по обслуживанию сервера.

Процедура

1. Отмените выполняющиеся процессы и сеансы, сделав следующее:
   a. Выберите в Центр операций на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   b. Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   c. Нажмите кнопку Отмена.
2. Остановите сервер с помощью команды HALT:

   ```
   halt
   ```

   Совет: Можно ввести команду halt из Центр операций, установив указатель мыши на значок Параметры и щелкнув по Построитель команд. Затем выберите сервер, введите `halt` и нажмите на клавишу ввода (Enter).

Ссылки, связанные с данной:
HALT (выключение сервера)

Подготовка к аварии и восстановление после аварии с использованием DRM

В IBM Spectrum Protect есть функция disaster recovery manager (DRM) для восстановления данных сервера и клиента при аварии.

DRM отслеживает перемещение носителей вне площадки и регистрирует эту информацию в базе данных IBM Spectrum Protect. DRM объединяет планы, сценарии и другую информацию в файле плана, который необходим для восстановления сервера IBM Spectrum Protect в случае, если произойдет авария или незапланированное отключение электричества. Если вас беспокоят возможные атаки вредоносных программ, включая программы, требующие выкупа, рассмотрите возможность использовать DRM, так как эта функция поможет вам восстановить серверы после атаки.

Ограничение: Поддержка DRM доступна только в продукте IBM Spectrum Protect Extended Edition.

- Файл плана аварийного восстановления
  В файле плана аварийного восстановления содержится информация, необходимая для восстановления сервера IBM Spectrum Protect до состояния, в котором он находился на момент выполнения последней операции резервного копирования базы данных, выполненной перед созданием плана.
- Восстановление данных сервера и клиента с использованим DRM
  Используйте функцию disaster recovery manager (DRM), чтобы восстановить данные сервера и клиента IBM Spectrum Protect, если произойдет авария.
- Тренировка по восстановлению после аварий
  Запланируйте отработку аварийного восстановления, чтобы подготовиться к аудиту, удостоверяющему возможность восстановления сервера IBM Spectrum Protect и гарантирующему, что можно восстановить данные и возобновить операции после перебоя с питанием. Отработка также поможет вам убедиться, что можно восстановить все данные и возобновить операции, прежде чем возникнет критическая ситуация.
- Восстановление базы данных
  Если у вас включена функция disaster recovery manager (DRM) и вы выполнили процедуру по подготовке к аварии, вы сможете восстановить базу данных после аварии. Если у вас не сконфигурирована функция DRM, вы все равно сможете восстановить базу данных при условии, что у вас есть необходимые файлы резервных копий.

Файл плана аварийного восстановления

В файле плана аварийного восстановления содержится информация, необходимая для восстановления сервера IBM Spectrum Protect до состояния, в котором он находился на момент выполнения последней операции резервного копирования базы данных, выполненной перед созданием плана.

План поделен на разделы, которые можно распределить по нескольким файлам. Каждый раздел содержит оператор begin и оператор end.

Табл. 1. Разделы файла плана аварийного восстановления

Раздел	**Информация в разделе**
SERVER.REQUIREMENTS	Задает требования к пространству хранения для базы данных и журнала восстановления сервера.
RECOVERY.INSTRUCTIONS.GENERAL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.GENERAL. Инструкции содержат стратегию восстановления, имена основных контактных лиц, обзор главных приложений, резервные копии которых были созданы на этом сервере, а также другие важные инструкции по восстановлению.
RECOVERY.INSTRUCTIONS.OFFSITE	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.OFFSITE. Инструкции задаяют имя и положение дистанционного хранилища, а также контактная информация администратора хранилища (например, имя и номер телефона).

Раздел	Информация в разделе
RECOVERY.INSTRUCTIONS.INSTALL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.INSTALL. Инструкции содержат указания по восстановлению сборки базового сервера и сведения о расположении резервных копий образа системы.
RECOVERY.INSTRUCTIONS.DATABASE	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.DATABASE. Инструкции содержат указания по подготовке к восстановлению базы данных. Например, можно указать инструкции по инициализации или загрузке резервных томов для автоматизированной библиотеки. Примеров этого раздела нет.
RECOVERY.INSTRUCTIONS.STGPOOL	Содержит инструкции, которые администратор ввел в файл, идентифицируемый префиксом RECOVERY.INSTRUCTIONS.STGPOOL. Инструкции содержат названия приложений и имена пулов хранения копий, содержащих резервные копии этих приложений. Примеров этого раздела нет.
RECOVERY.VOLUMES.REQUIRED	Позволяет получить список томов пула хранения резервных копий базы данных и копий, которые нужны для восстановления сервера. Том резервной копии базы данных добавляется в список, если он является частью самой последней последовательности резервных копий базы данных. Том пула хранения копий добавляется в список, если он не пуст и не отмечен как поврежденный (destroyed).
RECOVERY.DEVICES.REQUIRED	Содержит сведения об устройствах, необходимых для чтения резервных томов.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Содержит сценарий с командами, необходимыми для восстановления сервера.
RECOVERY.SCRIPT.NORMAL.MODE	Содержит сценарий с командами, необходимыми для восстановления первичных пулов хранения сервера.
DB.STORAGEPATHS	Задает каталоги для базы данных IBM Spectrum Protect.
LICENSE.REGISTRATION	Содержит макрокоманду для регистрации серверных лицензий.
COPYSTGPOOL.VOLUMES.AVAILABLE	Содержит макрокоманду, позволяющую отмечать тома пулов хранения копий, которые были перемещены в дистанционное хранилище, а затем возвращены в подключенное расположение. Эту информацию можно использовать в качестве руководства по командам администрирования. Можно также скопировать, изменить и запустить макрокоманду в файле. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.

Раздел	Информация в разделе
COPYSTGPOOL.VOLUMES.DESTROYED	Содержит макрокоманду, позволяющий пометить как недоступные тома пулов хранения копий, которые на момент аварии находились в подключенном расположении. Предполагается, что эти тома находятся в дистанционном хранилище и во время аварии не были повреждены. Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.DESTROYED	Содержит макрос, обозначающий находившиеся на момент аварии в подключенном расположении тома первичных пулов хранения как поврежденные (destroyed). Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.REPLACEMENT	Содержит макрокоманду для определения первичных пулов хранения замены. Эти сведения можно использовать в качестве руководства для ввода команд администрирования в командной строке; можно также скопировать их в файл, изменить его, а затем запустить макрокоманду. Эту макрокоманду вызывает сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
STGPOOLS.RESTORE	Содержит макрокоманду для восстановления первичных пулов хранения. Этот раздел можно использовать в качестве руководства, а административные команды вводить в командной строке. Можно также скопировать, изменить и запустить информацию в файле. Этот макрос запускается сценарием RECOVERY.SCRIPT.NORMAL.MODE.
VOLUME.HISTORY.FILE	Содержит копию сведений об хронологии томов на момент создания плана восстановления. Файл хронологии томов используется утилитой DSMSERV RESTORE DB, чтобы определить, какие тома необходимы для восстановления базы данных. Файл хронологии томов используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DEVICE.CONFIGURATION.FILE	Содержит копию данных о конфигурации устройств на момент создания плана восстановления. Файл конфигурации устройств используется утилитой DSMSERV RESTORE DB для чтения томов резервных копий базы данных. Файл конфигурации устройств используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DSMSERV.OPT.FILE	Содержит копию файла серверных параметров. Этот раздел используется сценарием RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
LICENSE.INFORMATION	Содержит копию результатов последнего аудита лицензий, а также условия соглашения о лицензии на сервер.
MACHINE.GENERAL.INFORMATION	Позволяет получить информацию о компьютере сервера, например, его расположение, которое необходимо, чтобы перестроить компьютер сервера. Этот раздел содержится в файле плана, если сведения о компьютерах были сохранены в базе данных при помощи команды DEFINE MACHINE с параметром ADSMSERVER=YES.

Раздел	Информация в разделе
MACHINE.RECOVERY.INSTRUCTIONS	Содержит инструкции по восстановлению для компьютера сервера. Этот раздел содержится в файле плана, если в базе данных были сохранены инструкции по восстановлению компьютера.
MACHINE.RECOVERY.CHARACTERISTICS	Содержит сведения о программных и аппаратных характеристиках сервера. Этот раздел содержится в файле плана, если характеристики компьютера сохранены в базе данных.
MACHINE.RECOVERY.MEDIA	Предоставляет информацию о носителях, необходимых для перестройки компьютера, содержащего сервер. Этот раздел содержится в файле плана, если сведения о носителях для восстановления сохранены в базе данных и связаны с компьютером, на котором расположен сервер.

Восстановление данных сервера и клиента с использованим DRM

Используйте функцию disaster recovery manager (DRM), чтобы восстановить данные сервера и клиента IBM Spectrum Protect, если произойдет авария.

Прежде чем начать

IBM Spectrum Protect настраивается для использования протокола Secure Sockets Layer (SSL) для аутентификации клиента/сервера. При запуске сервера создается файл цифрового сертификата, cert.kdb как часть процесса. В этом файле содержится открытый ключ сервера, который позволяет клиенту шифровать данные. Файл цифрового сертификата не может храниться в базе данных сервера, поскольку для Global Security Kit (GSKit) необходим отдельный файл в определённом формате.

1. Сохраните резервные копии файлов cert.kdb, cert.sth и cert256.arm.
2. Если и исходные файлы сертификатов, и все копии окажутся потеряны или повреждены, сгенерируйте новый файл сертификата.

Главный ключ шифрования хранится в новой базе данных ключей, управляемой комплектом GSKit, dsmkeydb.kdb. Если на сервере есть существующий главный ключ шифрования, этот главный ключ шифрования будет перенесен из файла dsmserv.pwd в базу данных ключей, dsmkeydb.kdb. Сохраните резервные копии файлов dsmkeydb.kdb и dsmkeydb.sth. Можно сконфигурировать команду BACKUP DB для резервного копирования главного ключа шифрования или можно самостоятельно создать резервную копию файлов dsmkeydb.kdb и dsmkeydb.sth вручную. Без главного ключа шифрования произвести восстановление после аварии будет невозможно.

1. Сохраните резервные копии файлов dsmkeydb.kdb и dsmkeydb.sth.

Процедура

1. Получите последний план восстановления.
2. Ознакомьтесь с этапами восстановления, описанными в разделе плана RECOVERY.INSTRUCTIONS.GENERAL.
3. Разбейте разделы файла плана по отдельным файлам, чтобы получить общие предварительные инструкции, сценарии восстановления сервера IBM Spectrum Protect и инструкции по восстановлению клиентов.
4. Получите все необходимые тома восстановления (как указано в плане) из хранилища.
5. Проверьте файл конфигурации устройств и убедитесь, что конфигурация оборудования на площадке восстановления совпадает с конфигурацией на исходной площадке. При наличии любых изменений следует соответствующим образом обновить файл конфигурации устройств. Ниже приведены примеры изменений, для которых нужно изменить конфигурацию:
   - Различные имена устройств.
   - Для автоматизированных библиотек - требование вручную разместить тома резервных копий базы данных в автоматизированной библиотеке и обновить данные о конфигурации для идентификации элементов библиотеки. Это позволит серверу находить расположение требуемых томов резервных копий базы данных.
6. Настройте замену оборудования для сервера IBM Spectrum Protect, включая операционную систему и установку базового выпуска IBM Spectrum Protect.

7. Запустите сценарий восстановления сервера IBM Spectrum Protect из плана восстановления. Разделы RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE и RECOVERY.SCRIPT.NORMAL.MODE содержат выполняемые файлы команд, которые можно использовать для управления восстановлением сервера IBM Spectrum Protect, вызывая другие файлы команд, сгенерированные в плане. Сценарий RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE восстанавливает сервер до той точки, в которой клиенты могут начать, восстановление непосредственно с томов пулов хранения копий.
8. Восстановите первичные пулы хранения, используя сценарий RECOVERY.SCRIPT.NORMAL.MODE.
9. Запустите операции восстановления клиента в соответствии с порядком приоритетов, заданным в высокоуровневом планировании.

Дальнейшие действия

Теперь сервер IBM Spectrum Protect можно использовать для выполнения обычных операций сервера. Убедитесь, что запланированы все необходимые операции. Инструкции смотрите в разделах Как задать расписания для операций по обслуживанию сервера и Планирование операций резервного копирования и архивирования.

Ссылки, связанные с данной:

PREPARE (создание файла с планом восстановления)

Информация, связанная с данной:

Исправление и восстановление данных в пулах хранения каталогов-контейнеров

Тренировка по восстановлению после аварий

Запланируйте отработку аварийного восстановления, чтобы подготовиться к аудиту, удостоверяющему возможность восстановления сервера IBM Spectrum Protect и гарантирующему, что можно восстановить данные и возобновить операции после перебоя с питанием. Отработка также поможет вам убедиться, что можно восстановить все данные и возобновить операции, прежде чем возникнет критическая ситуация.

Прежде чем начать

Выполните следующие задачи:

- Регулярно планируйте операции по управлению, защите и обслуживанию сервера. Дополнительную информацию о планировании смотрите в разделе Как задать расписания для операций по обслуживанию сервера. Убедитесь, что вы запланировали следующие задачи:
  - Резервное копирование базы данных.
  - Перемещение носителей вне площадки.
  - Резервное копирование файла конфигурации устройств, файла хронологии томов и файла опций сервера dsmserv.opt.
  - **Необязательно:** Ввод команды PREPARE для создания файла плана аварийного восстановления.

  Совет:

  При вводе команды PREPARE функция IBM Spectrum Protectdisaster recovery manager (DRM) создает одну копию файла плана аварийного восстановления.

  Управлять аварийным восстановлением вне площадки можно, не используя DRM, однако DRM помогает консолидировать планы, сценарии и другую информацию, которая требуется при восстановлении после аварий.

  Для безопасности создайте создать несколько копий плана. Например, сохраните копии в печатном виде, на флэш-накопителе USB, на дисковом пространстве вне площадки или на удаленном сервере. Файл плана аварийного восстановления ежедневно перемещается за пределы площадки с использованием лент. Дополнительную информацию о DRM смотрите в разделе Подготовка к аварии и восстановление после аварии с использованием DRM.

- Сконфигурируйте следующие ресурсы на площадке аварийного восстановления:
  1. Сервер IBM Spectrum Protect восстановления. Сервер на площадке аварийного восстановления должен относиться к тому же уровню, что и сервер на производственной площадке.
  2. Ленточную библиотеку для хранения носителей, поставляемых с производственной площадки. Дополнительную информацию о расположениях восстановления вне площадки смотрите в разделе Хранение данных вне площадки.
  3. Дисковое пространство хранения для базы данных, архивного журнала, активных журналов и пулов хранения.
  4. Клиенты для проверки операций по восстановлению.

Об этой задаче

Почаще проверяйте план аварийного восстановления и возможность восстановления сервера IBM Spectrum Protect в среде, аналогичной производственной среде.

Процедура

1. Убедитесь, что ленты доступны на площадке. Введите команду QUERY LIBVOLUME, чтобы идентифицировать тома, активируемые в автоматизированной библиотеке.
2. Создайте резервную копию базы данных на лентах на площадке, выполнив следующие шаги:
    a. На странице Серверы в компоненте Центр операций выберите сервер, для базы данных которого вы хотите создать резервную копию.
    b. Щелкните по Резервное копирование и выполните инструкции в окне Резервное копирование базы данных.
3. Скопируйте в домашний каталог сервера на площадке восстановления следующие файлы:
    - Файл плана аварийного восстановления
    - Файл хронологии тома
    - Файл конфигурации устройств
    - Необязательно: файл опций сервера dsmserv.opt
4. Переместите ленту в расположение восстановления вне площадки.
5. Восстановите базу данных сервера, используя утилиту DSMSERV RESTORE DB на сервере восстановления. Дополнительную информацию о восстановлении базы данных сервера, смотрите раздел Восстановление базы данных.
6. Введите команду UPDATE VOLUME и задайте параметр ACCESS=DESTROYED, чтобы указать, что нужно восстановить весь том.
7. На сервере восстановления восстановите тома пула хранения при помощи команды RESTORE STGPOOL.

Дальнейшие действия

Убедитесь, что вы можете получить доступ к данным в библиотеке, произведя аудит ленточного тома в восстановленном пуле хранения, чтобы удостовериться, что данные не противоречивы. Чтобы произвести аудит ленточного тома, введите команду AUDIT VOLUME. Чтобы обеспечить более высокую производительность, произведите аудит только восстановленных данных.

Задачи, связанные с данной:

Аудит перечня томов в библиотеке

Ссылки, связанные с данной:

AUDIT VOLUME (проверка информации о томе пула хранения, содержащейся в базе данных)

DSMSERV RESTORE DB (восстановление базы данных)

RESTORE STGPOOL (восстановление данных в пуле хранения)

Восстановление базы данных

Если у вас включена функция disaster recovery manager (DRM) и вы выполнили процедуру по подготовке к аварии, вы сможете восстановить базу данных после аварии. Если у вас не сконфигурирована функция DRM, вы все равно сможете восстановить базу данных при условии, что у вас есть необходимые файлы резервных копий.

Прежде чем начать

Если каталоги базы данных и журнала восстановления потеряны, то создайте их заново, прежде чем вводить серверную утилиту DSMSERV RESTORE DB.

Об этой задаче

Вы можете восстановить базу данных до наиболее актуального состояния или на указанный момент времени. Чтобы восстановить базу данных на момент, когда она была потеряна, восстановите ее до самой последней версии. Ограничения:

- Чтобы восстановить базу данных до ее последней версии, нужно найти каталог архивного журнала. Если вы не сможете найти каталог, вам удастся восстановить базу данных только на конкретный момент времени.
- Протокол Secure Sockets Layer (SSL) нельзя использовать для операции восстановления баз данных.

- Вы не сможете восстановить базу данных сервера, если уровень выпуска резервной копии базы данных отличается от уровня выпуска восстанавливаемого сервера. Например, если вы используете сервер версии 8.1 и попытаетесь восстановить базу данных версии 7.1, произойдет ошибка.

Процедура

Чтобы восстановить базу данных, используйте серверную утилиту DSMSERV RESTORE DB. Выберите один из следующих методов в зависимости от того, какую версию базы данных вы хотите восстановить:

- Восстановить базу данных до самой последней версии. Например, введите следующую команду:

  ```
  dsmserv restore db
  ```

- Восстановить базу данных на определенный момент времени. Например, чтобы восстановить базу данных на момент создания набора резервных копий от 19 апреля 2017 г., используйте следующую команду:

  ```
  dsmserv restore db todate=04/19/2017
  ```

Ссылки, связанные с данной:
DSMSERV RESTORE DB (восстановление базы данных)

Документация по решению в файлах PDF

Вы можете скачать файлы PDF с решениями для защиты данных IBM Spectrum Protect.

Для решений по защите данных IBM Spectrum Protect есть следующие файлы PDF:

- Введение в решения по защите данных
- Руководство по дисковому решению с одной площадкой
- Руководство по дисковому решению с несколькими площадками
- Руководство по решению на лентах

Чтобы узнать о дополнительных предварительно построенных файлах PDF документации по серверу IBM Spectrum Protect, смотрите полный список.

Серверы IBM Spectrum Protect

Серверы IBM Spectrum Protect хранят резервные, архивные и перенесенные данные для клиентов резервного копирования и архивирования и других компонентов IBM Spectrum Protect и IBM Spectrum Protect Snapshot, и управляют этими данными.

- Что нового
  Узнайте о новых функциях и обновлениях серверных компонентов в IBM Spectrum Protect версии 8.1.
- Установка и обновление
  Вы можете установить или обновить отдельные компоненты или несколько компонентов в среде вашего предприятия. Доступна документация по решению, которая поможет вам выбрать наилучшее практическое решение на основе ваших бизнес-требований, а затем установить, сконфигурировать, отслеживать решение и работать с ним.
- Конфигурирование серверов
  Чтобы выполнить задачи по конфигурированию для сервера, ознакомьтесь с доступной документацией.
- Серверные команды, опции и утилиты
  Используйте команды для администрирования и конфигурирования сервера, опции - для настройки сервера и утилиты - для выполнения специализированных задач, когда сервер не работает.
- Документация по серверу в файлах PDF
  Вы можете скачать файлы PDF с документацией по IBM Spectrum Protect.

Что нового

Узнайте о новых функциях и обновлениях серверных компонентов в IBM Spectrum Protect версии 8.1.

Совет: Чтобы посмотреть видеоролики о новых функциях и обновлениях, смотрите раздел Видеобиблиотека.
Чтобы прочитать о новых функциях и обновлениях, следуйте ссылкам в таблице.

Выпуск	Новые функции и обновления
V8.1.5	Сервер • Снижение затрат на пулы хранения облачных контейнеров за счет высвобождения пространства • Управление средой хранения поможет вам обеспечить соответствие стратегиям совместимости General Data Protection Regulation • Генерирование статистики дедупликации данных для указанных узлов и файловых пространств • Планирование операций аудита, позволяющих выявить поврежденные файлы в пуле хранения Центр операций Обновления компонента Центр операций, включая обнаружение программ-вымогателей
V8.1.4	Сервер • Увеличение минимальной длины паролей по умолчанию для усовершенствования защиты • Воспользуйтесь преимуществами автоматического обмена сертификатами между агентами хранения, клиентами библиотеки и серверами менеджеров библиотек • Оптимизация защиты с использованием сертификатов с подписями SHA256 • Как указать, нужно ли принудительно применять требования FIPS 140-2 при шифровании • Сокращение фрагментации данных при перемещении содержимого контейнеров пулов хранения Центр операций Обновления Центра операций
V8.1.3	Сервер • Использование облачных слоев для долгосрочного хранения данных • Установка IBM Spectrum Protect в Linux Ubuntu Server LTS • Усовершенствование защиты среды хранения • Меры, помогающие защитить систему от программ, требующих выкуп Центр операций Обновления Центра операций
V8.1.2	Сервер • Резервное копирование данных в Microsoft Azure, систему хранения объектов на основе облака • Шифрование данных клиента в пуле хранения каталога-контейнера • Создайте резервную копию файл-сервера NAS в пуле хранения каталога-контейнера • Установка IBM Spectrum Protect в операционной системе Linux on Power Systems (с прямым порядком байтов) • Защитите среду хранения за счет улучшенного протокола защиты • Оптимизируйте защиту с использованием автоматически генерируемого главного ключа шифрования • Сконфигурируйте среду хранения, используя Руководство по ленточным решениям • Запланируйте автоматические обновление клиентов резервного копирования и архивирования • Опции сервера, команды и параметры, которые устарели и поддержка которых прекращена Центр операций Обновления Центра операций

Выпуск	Новые функции и обновления
V8.1.1	Сервер • Установить IBM Spectrum Protect в операционной системе Linux on Power Systems (с прямым порядком байтов) • Установить IBM Spectrum Protect в операционной системе Microsoft Windows Server 2016 • Использовать библиотеку Quantum Scalar i6 • Ознакомиться с устраненными проблемами Центр операций • Ознакомиться с устраненными проблемами
V8.1	Сервер • Представляем IBM Spectrum Protect • Защищенная связь с использованием протокола TLS 1.2 • Преобразование ленточного пула хранения в пул хранения контейнера • Обновление программного обеспечения для менеджера базы данных сервера • Команда REGISTER NODE больше не создает ID пользователя-администратора по умолчанию • Оптимизация аутентификации пользователей в базе данных Active Directory • Повышенная гибкость при защите и высвобождении ленточных томов в пулах хранения контейнеров-копий • Поддерживаемые операционные системы • Отслеживание системы без использования SNMP Центр операций Обновления Центра операций

- Обновления Центра операций
  В Центр операций IBM Spectrum Protect версии 8.1.5 появились новые функции.
- Обновления сервера IBM Spectrum Protect
  На сервере IBM Spectrum Protect версии 8.1.5 есть новые функции и другие изменения.
- Замечания по выпуску для серверных компонентов версии 8.1
  Для компонентов V8.1 появились замечания по выпуску.
- Файлы Readme для серверных компонентов версии 8.1
  Файлы readme для пакетов Fix Pack версии 8.1 опубликованы на сайте программной поддержки IBM. Обновления могут быть доступны для серверных компонентов, в том числе для самого сервера, поддержки устройств и Центр операций.

Обновления Центра операций

В Центр операций IBM Spectrum Protect версии 8.1.5 появились новые функции.

Доступны следующие новые функции:

- Уведомления системы защиты о потенциальных атаках программ-вымогателей. После каждого сеанса резервного копирования клиента анализируются статистические показатели, чтобы найти признаки заражения программой-вымогателем. Если есть такие признаки, в Центре операций будет показано предупреждающее сообщение. Используя новую страницу Уведомления защиты, можно просмотреть сведения для каждого уведомления защиты. Эта информация поможет определить, заражен ли клиент программой-вымогателем, или уведомление является ложноположительным.
- Высвобождение пространства в пулах хранения облачных контейнеров, что помогает сократить расходы на хранение. При удалении данных или при окончании их срока хранения в пулах хранения облачных контейнеров происходит фрагментация. В результате этого в облачном контейнере есть занятое, но неиспользуемое пространство. Теперь можно задать порог для высвобождения этого пространства. Выбирая порог высвобождения, можно увидеть оценку экономии пространства, которой можно добиться. Также можно увидеть оценку числа требований о перемещении данных и объем данных, которые нужно отправлять и принимать. Эти оценки можно использовать, чтобы принять решение относительно порога высвобождения, который будет экономически наиболее выгодным при взимаемой вашим облачным провайдером плате за хранение и перемещение данных.

Дополнительную информацию об этих усовершенствованиях смотрите в справке для компонента Центр операций.

Задачи, связанные с данной:
Высвобождение облачных контейнеров
Ссылки, связанные с данной:
Ежедневный контрольный список

Обновления сервера IBM Spectrum Protect

На сервере IBM Spectrum Protect версии 8.1.5 есть новые функции и другие изменения.

- Снижение затрат на пулы хранения облачных контейнеров за счет высвобождения пространства
  Работая с IBM Spectrum Protect версии 8.1.5, можно использовать новую функцию высвобождения облака для высвобождения пространства в пулах хранения облачных контейнеров. Можно переместить данные из большего, фрагментированного облачного контейнера в меньший, используемый в более полной мере облачный контейнер. Это поможет вам сократить затраты на использование хранилища объектов для пулов хранения облачных контейнеров.
- Управление средой хранения поможет вам обеспечить соответствие стратегиям совместимости General Data Protection Regulation
  Нормативы General Data Protection Regulation (GDPR), вступившие в силу 25 мая 2018 г., направлены на то, чтобы гармонизировать требования к конфиденциальности данных в Европейском Союзе (ЕС). Можно использовать существующие функции IBM Spectrum Protect и усовершенствования, включенные в IBM Spectrum Protect версии 8.1.5, которые помогут вам управлять средой хранения с учетом стратегий совместимости с GDPR.
- Генерирование статистики дедупликации данных для указанных узлов и файловых пространств
  Используя IBM Spectrum Protect версии 8.1.5, можно периодически генерировать статистику дедупликации данных для указанных узлов, групп узлов и файловых пространств. При помощи команды DEFINE STGRULE, можно генерировать статистику каждый день в одно и то же время суток либо можно делать это с заданными интервалами.
- Планирование операций аудита, позволяющих выявить поврежденные файлы в пуле хранения
  Используя IBM Spectrum Protect версии 8.1.5, можно запланировать операции аудита, позволяющие выявить поврежденные файлы в пуле хранения.

Снижение затрат на пулы хранения облачных контейнеров за счет высвобождения пространства

Работая с IBM Spectrum Protect версии 8.1.5, можно использовать новую функцию высвобождения облака для высвобождения пространства в пулах хранения облачных контейнеров. Можно переместить данные из большего, фрагментированного облачного контейнера в меньший, используемый в более полной мере облачный контейнер. Это поможет вам сократить затраты на использование хранилища объектов для пулов хранения облачных контейнеров.

При удалении данных или при окончании их срока хранения в пулах хранения облачных контейнеров происходит фрагментация. Чтобы высвободить неиспользуемое пространство в облачном контейнере, можно запланировать ежедневную операцию высвобождения облака, введя команду сервера DEFINE STGRULE с параметром ACTIONTYPE=RECLAIM. Когда неиспользуемое пространство в облачном контейнере достигнет заданного вами процента, данные будут перемещены в контейнер меньшего размера. Вы можете запланировать разовую операцию высвобождения, введя команду MOVE CONTAINER с параметром по умолчанию DEFRAG=YES.

Либо можно использовать графический пользовательский интерфейс центра операций чтобы запланировать операции высвобождения облачного пространства и оценить экономию пространства для архивирования.

Задачи, связанные с данной:
Высвобождение облачных контейнеров
Ссылки, связанные с данной:
DEFINE STGRULE (задать правило для высвобождения пулов хранения облачных контейнеров)
MOVE CONTAINER (Переместить контейнер)
Обновления Центра операций

Управление средой хранения поможет вам обеспечить соответствие стратегиям совместимости General Data Protection Regulation

Нормативы General Data Protection Regulation (GDPR), вступившие в силу 25 мая 2018 г., направлены на то, чтобы гармонизировать требования к конфиденциальности данных в Европейском Союзе (ЕС). Можно использовать существующие функции IBM Spectrum Protect и усовершенствования, включенные в IBM Spectrum Protect версии 8.1.5, которые помогут вам управлять средой хранения с учетом стратегий совместимости с GDPR.

В IBM Spectrum Protect версии 8.1.5 включены усовершенствования, позволяющие вести журнал аудита, который можно использовать для отслеживания удалений с сервера. Эти усовершенствования вместе с существующими функциями IBM Spectrum Protect для удаления данных на сервере и клиенте резервного копирования и архивирования, могут помочь вам обеспечить соответствие Статье 17 GDPR, "Right to erasure (right to be forgotten)" (Право на уничтожение (право забыть)). Кроме того, такие существующие функции как Transport Layer Security (TLS), которые позволяют защитить обмен данными, могут помочь обеспечить соответствие Статье 32, "Security of processing" (Защита обработки).

Более подробную информацию о функциях IBM Spectrum Protect, которые могут обеспечить поддержку стратегий совместимости GDPR, смотрите в техническом замечании 22014168.

Генерирование статистики дедупликации данных для указанных узлов и файловых пространств

Используя IBM Spectrum Protect версии 8.1.5, можно периодически генерировать статистику дедупликации данных для указанных узлов, групп узлов и файловых пространств. При помощи команды DEFINE STGRULE, можно генерировать статистику каждый день в одно и то же время суток либо можно делать это с заданными интервалами.

Чтобы сгенерировать статистику разовым образом, можно ввести команду GENERATE DEDUPSTATS, после которой запустить команду QUERY DEDUPSTATS. Начиная с V8.1.5, можно ограничить выходную информацию обеих команд, задав списки узлов, группы узлов и файловые пространства. Кроме того, запуская команду QUERY DEDUPSTATS, можно получить сводный отчет о статистике для заданного набора узлов, групп узлов и файловых пространств.
Задачи, связанные с данной:
Как задать правило хранения для генерирования статистики дедупликации данных
Ссылки, связанные с данной:
DEFINE STGRULE (задать правило для генерирования статистики дедупликации данных)
GENERATE DEDUPSTATS (Сгенерировать статистику дедупликации данных)
QUERY DEDUPSTATS (Запросить статистику дедупликации данных)

Планирование операций аудита, позволяющих выявить поврежденные файлы в пуле хранения

Используя IBM Spectrum Protect версии 8.1.5, можно запланировать операции аудита, позволяющие выявить поврежденные файлы в пуле хранения.

Чтобы запланировать операции аудита, используйте команду DEFINE STGRULE с параметром ACTIONTYPE=AUDIT. Если оставить для параметра DELAY значение по умолчанию, равное 7, операция аудита будет выполняться еженедельно в одно и то же время.
Задачи, связанные с данной:
Аудит пула хранения
Ссылки, связанные с данной:
DEFINE STGRULE (задать правило для аудита пулов хранения)
UPDATE STGRULE (обновить правило для аудита пула хранения)

Замечания по выпуску для серверных компонентов версии 8.1

Для компонентов V8.1 появились замечания по выпуску.

- Замечания по выпуску для сервера IBM Spectrum Protect версии 8.1
  Появился сервер IBM Spectrum Protect V8.1. Описывается совместимость, установка и другие вопросы, связанные с началом работы.
- Замечания по выпуску для Центр операций версии 8.1
  Центр операций - это веб-интерфейс, который можно использовать для управления вашей средой IBM Spectrum Protect. Замечания по выпуску содержат ссылки на объявление о продукте, известные проблемы, требования к системе, инструкции по установке и обновления.

- Замечания по выпуску для поддержки устройств IBM Spectrum Protect версии 8.1
  Доступна поддержка устройств IBM Spectrum Protect для версии 7.1. Описывается совместимость, установка и другие вопросы, связанные с началом работы.

Замечания по выпуску для сервера IBM Spectrum Protect версии 8.1

Появился сервер IBM Spectrum Protect V8.1. Описывается совместимость, установка и другие вопросы, связанные с началом работы.

Содержание

Описание

IBM Spectrum Protect предоставляет возможности автоматизации, централизованного планирования и использования политики для управления процессами резервного копирования, архивирования и управления пространством для файл-серверов, рабочих станций, виртуальных машин и прикладных программ.

Авторизованный отчет анализа программы (authorized program analysis report, APAR) - это требование исправления дефекта в поддерживаемом выпуске программы, поставляемой IBM. Список APAR, для которых были устранены соответствующие ошибки, смотрите в документе Исправленные APAR для сервера IBM Spectrum Protect версии 8.1.

Объявление

Объявление о семействе продуктов IBM Spectrum Protect V8.1 содержит следующую информацию:

- Подробное описание продукта включая описание новых функций
- Заявление о позиционировании продукта
- Международная информация о совместимости

Для поиска объявления о продукте выполните следующие действия:

1. Перейдите на сайт объявлений о продуктах.
2. В поле Search for введите идентификатор продукта (PID) для вашего продукта. PID для IBM Spectrum Protect - 5725-W98.
3. В поле Information Type выберите Announcement letters и нажмите кнопку Search.
4. В списке Search in выберите Product Number.
5. Необязательно: На панели Refine Your Search в левой части окна выберите регион, в котором вы находитесь.
6. В разделе Sort by выберите Newest first.

Совместимость с предыдущими версиями

Информацию о совместимости с более ранними версиями смотрите в документе Особенности совместимости и обновления сервера/клиента IBM Spectrum Protect.

Требования к системе

Информацию о требованиях к системе смотрите в документе Поддерживаемые операционные системы IBM Spectrum Protect.

Установка и обновление IBM Spectrum Protect

Инструкции по установке сервера смотрите в процедуре для своей операционной системы.

IBM AIX
: Установка сервера

Linux
: Установка сервера

Microsoft Windows
: Установка сервера

Инструкции по обновлению смотрите в разделе Обновление до V8.1.

Обновления, ограничения и известные проблемы

Обновления содержат новую информацию о продукте или новых возможностях продукта, которые стали доступны после выпуска продукта. Обновления, информация об ограничениях и известных проблемах представлена в форме технических замечаний в информационной базе поддержки на портале поддержки IBM®. Производя поиск в информационной базе данных, вы сможете найти обходные пути или способы устранения проблем.

Обновления
: **Команда REGISTER NODE больше не создает ID пользователя-администратора по умолчанию**
Начиная с IBM Spectrum Protect V8.1, команда REGISTER NODE не создает автоматически ID пользователя-администратора, соответствующий имени узла. Это обновление продукта может повлиять на процесс регистрации клиентских узлов, включая, но не ограничиваясь таковыми, узлы клиентов резервного копирования и архивирования IBM Spectrum Protect. В некоторых случаях вам может потребоваться создать ID пользователя-администратора, задав параметр USERID в команде REGISTER NODE. Информацию о типах клиентов, на которые это влияет, смотрите в документе техническое замечание 7048963.

  Последние обновления смотрите в документе Обновления IBM Spectrum Protect V8.1.

Ограничения и известные проблемы
: На момент публикации никакой информации об ограничениях или известных проблемах не было.

  Последние ограничения и известные проблемы с дополнительными пунктами смотрите в документе Ограничения и известные проблемы для IBM Spectrum Protect V8.1.

Замечания по выпуску для Центр операций версии 8.1

Центр операций - это веб-интерфейс, который можно использовать для управления вашей средой IBM Spectrum Protect. Замечания по выпуску содержат ссылки на объявление о продукте, известные проблемы, требования к системе, инструкции по установке и обновления.

Содержание

Описание

Центр операций можно использовать для следующих действий:

- Идентификация потенциальных проблем с вашей средой IBM Spectrum Protect
- Мониторинг ключевых аспектов среды хранения: оповещений, клиентов, серверов, политик, пулов хранения и устройств хранения
- Регистрация клиентов
- Добавление отслеживаемых серверов
- Резервное копирование баз данных серверов, клиентов и пулов хранения
- Начальный перенос пула хранения и высвобождение пространства
- Назначение оповещений администраторам и закрытие оповещений
- Просмотр и отмена процессов сервера и сеансов клиента
- Изменение параметров клиента, сервера, пула хранения и устройства хранения
- Создание и управление расписаниями клиентов и просмотр административных расписаний
- Преобразование первичных пулов хранения в пулы хранения контейнеров

- Копирование пулов хранения каталогов-контейнеров на ленту
- Конфигурирование репликации
- Изменение параметров политики
- Списание клиентов и деактивация данных
- Создание электронных отчетов
- Просмотр фронтальной и внутренней емкости хранения, чтобы отслеживать соответствие лицензии
- Передача на выполнение команд серверам IBM Spectrum Protect

Авторизованный отчет анализа программы (authorized program analysis report, APAR) - это требование исправления дефекта в поддерживаемом выпуске программы, поставляемой IBM. Список APAR, для которых были устранены соответствующие ошибки, смотрите в документе Исправленные APAR для центра операций IBM Spectrum Protect версии 8.1.

Объявление

Центр операций - это часть семейства продуктов IBM Spectrum Protect V8.1. Объявление об этих продуктах содержит следующую информацию:

- Подробное описание продукта включая описание новых функций
- Заявление о позиционировании продукта
- Международная информация о совместимости

Для поиска объявления о продукте выполните следующие действия:

1. Перейдите на сайт объявлений о продуктах.
2. В поле Search for введите идентификатор продукта (PID) для вашего продукта. PID для IBM Spectrum Protect - 5725-W98.
3. В поле Information Type выберите Announcement letters и нажмите кнопку Search.
4. В списке Search in выберите Product Number.
5. Необязательно: На панели Refine Your Search в левой части окна выберите регион, в котором вы находитесь.
6. В разделе Sort by выберите Newest first.

Совместимость с сервером IBM Spectrum Protect.

Информацию о совместимости смотрите в документе Совместимость сервера и центра операций IBM Spectrum Protect.

Требования к системе

Информацию о требованиях к системе смотрите в документе Требования центра операций IBM Spectrum Protect к программным и аппаратным средствам.

Установка или обновление Центра операций

Инструкции по установке или обновлению существующей версии Центра операций смотрите в разделе Установка и обновление Центра операций.

Обновления, ограничения и известные проблемы

Обновления содержат новую информацию о продукте или новых возможностях продукта, которые стали доступны после выпуска продукта. Обновления, информация об ограничениях и известных проблемах представлена в форме технических замечаний в информационной базе поддержки на портале поддержки IBM®. Производя поиск в информационной базе данных, вы сможете найти обходные пути или способы устранения проблем.

Обновления

Новейший список обновлений смотрите в документе Результаты поиска обновлений для Центр операций V8.1.

Ограничения и известные проблемы

- Список ограничений и известных проблем смотрите в документе Ограничения и известные проблемы Центр операций V8.1.
- Чтобы найти дополнительную информацию об известных проблемах, которые могли стать известными после выпуска продукта, смотрите документ Результаты поиска известных проблем в Центр операций V8.1.

Замечания по выпуску для поддержки устройств IBM Spectrum Protect версии 8.1

Доступна поддержка устройств IBM Spectrum Protect для версии 7.1. Описывается совместимость, установка и другие вопросы, связанные с началом работы.

Содержание

Описание

Этот документ содержит информацию о драйверах устройств IBM Spectrum Protect версии 8.1.

Авторизованный отчет анализа программы (authorized program analysis report, APAR) - это требование исправления дефекта в поддерживаемом выпуске программы, поставляемой IBM. Список APAR, для которых были устранены соответствующие ошибки, смотрите в документе Исправления APAR в драйвере устройств IBM Spectrum Protect версии 8.1.

Объявление

Объявление о поддержке устройств IBM Spectrum Protect для версии 8.1 входит в состав объявления о семействе продуктов IBM Spectrum Protect. Объявление об этих продуктах содержит следующую информацию:

- Подробное описание продукта включая описание новых функций
- Заявление о позиционировании продукта
- Международная информация о совместимости

Для поиска объявления о продукте выполните следующие действия:

1. Перейдите на сайт объявлений о продуктах.
2. В поле Search for введите идентификатор продукта (PID) для вашего продукта. PID для IBM Spectrum Protect - 5725-W98.
3. В поле Information Type выберите Announcement letters и нажмите кнопку Search.
4. В списке Search in выберите Product Number.
5. Необязательно: На панели Refine Your Search в левой части окна выберите регион, в котором вы находитесь.
6. В разделе Sort by выберите Newest first.

Поддерживаемые устройства

Информацию о поддерживаемых устройствах и аппаратном обеспечении для систем IBM AIX и Microsoft Windows смотрите в публикации Поддерживаемые устройства для AIX и Windows.

Информацию о поддерживаемых устройствах и аппаратном обеспечении для систем Linux смотрите в документе Поддерживаемые устройства для Linux.

Требования драйверов устройств

Требования к адаптеру шины хоста
: Чтобы добиться наилучших результатов, подключайте к системе ленточные устройства и ленточные библиотеки, используя их собственный адаптер шины хоста. Не используйте адаптер шины хоста совместно с другими типами устройств, такими как диски или дисководы компакт-дисков.

Максимальное число устройств, поддерживаемых драйвером IBM Spectrum Protect
: Информацию о максимальном числе устройств, которые драйверы устройств IBM Spectrum Protect способны поддерживать в каждой операционной системе, смотрите в техническом замечании technote 1364225.

Поддержка устройств Serial Attached SCSI (SAS)

Устройства SAS можно использовать в некоторых операционных системах и архитектурах. Информацию об операционных системах и архитектурах для устройств SAS смотрите в техническом замечании 1396706.

Запуск промежуточного драйвера IBM Spectrum Protect (passthru) от имени пользователя, не являющегося пользователем root, в операционных системах Linux

Информацию о том, как пользователь, не являющийся пользователем root, может использовать устройства с промежуточным драйвером IBM Spectrum Protect в Linux, смотрите в техническом замечании 1321130. Используйте опцию -g или -a утилиты autoconf устройства, чтобы пользователи, отличные от пользователя root, могли использовать устройства с промежуточным драйвером IBM Spectrum Protect. Используйте опцию -g, чтобы добавить разрешения на чтение и запись для групп в файлы устройств типового драйвера SCSI (generic driver, sg). Используйте опцию -a, чтобы добавить в файлы устройств sg разрешения на чтение и запись для всех пользователей.

Информация, касающаяся библиотек

- Для работы с библиотекой, содержащей более четырех накопителей или более 48 слотов хранения, требуется IBM Spectrum Protect Extended Edition.
- Адреса элементов для слотов хранения могут не коррелироваться напрямую с номерами слотов хранения. Это важный факт, так как сервер IBM Spectrum Protect всегда ссылается на слоты хранения, используя адреса элементов, а не номера слотов хранения. Смотрите адреса элементов на странице конфигурации библиотеки для каждой библиотеки.
- В случае библиотеки с несколькими накопителями для выполнения команд DEFINE и UPDATE DRIVE требуется адрес элемента накопителя. Однако, если библиотека сообщает серийные номера накопителей, вы можете указать опцию ELEMENT=AUTODETECT, и адрес элемента не потребуется.
- Чтобы узнать, как сконфигурировать чейнджер и каждый накопитель в библиотеке по отдельности, смотрите раздел Конфигурирование устройств хранения и управление ими.

Обновления, ограничения и известные проблемы

Обновления

Некоторые устройства, которые поддерживались в предыдущих выпусках IBM Spectrum Protect, не поддерживаются сервером IBM Spectrum Protect V8.1. Последний список поддерживаемых устройств смотрите по следующим ссылкам:

- Поддерживаемые устройства для AIX и Windows
- Поддерживаемые устройства для Linux

Информацию о последних обновлениях, ограничениях и известных проблемах (включая дополнительные элементы) смотрите в документе Обновления, ограничения и известные проблемы для поддержки устройств IBM Spectrum Protect V8.1.

Файлы Readme для серверных компонентов версии 8.1

Файлы readme для пакетов Fix Pack версии 8.1 опубликованы на сайте программной поддержки IBM. Обновления могут быть доступны для серверных компонентов, в том числе для самого сервера, поддержки устройств и Центр операций.

Смотрите файлы readme для пакетов Fix Pack сервера IBM Spectrum Protect V8.1

Установка и обновление

- Реализация решения IBM Spectrum Protect
  Если вы внедряете новую среду сервера IBM Spectrum Protect, рассмотрите возможность реализовать наилучшую практическую конфигурацию.
- Установка и обновление сервера
  Сервер IBM Spectrum Protect предоставляет клиентам услуги резервного копирования, архивирования и управления пространством. Вы можете установить или обновить один или несколько серверов в среде вашего предприятия.
- Установка и обновление Центра операций
  Центр операций - это веб-интерфейс для управления средой хранения.

Реализация решения IBM Spectrum Protect

Если вы внедряете новую среду сервера IBM Spectrum Protect, рассмотрите возможность реализовать наилучшую практическую конфигурацию.

Доступна документация по решению IBM Spectrum Protect, которая поможет вам выбрать наилучшее практическое решение на основе ваших бизнес-требований, а затем установить, сконфигурировать, отслеживать решение и работать с ним.

Дополнительные сведения смотрите в разделе Выбор решения IBM Spectrum Protect.

Доступность функций по операционным системам

Большинство функций IBM Spectrum Protect доступны во всех операционных системах, которые поддерживаются для сервера.

В следующей таблице галочка указывает, что функция доступна.

Табл. 1. Доступность функций IBM Spectrum Protect по операционным системам

Функция	**IBM® AIX**	**Linux x86_64**	**Linux on System z**	**Linux on Power Systems (с обратным порядком байт)**	**Microsoft Windows**
Технология Aspera Fast Adaptive Secure Protocol (FASP): Оптимизировать передачу данных на удаленном сервере.		✓ 1			
Облачное хранение с использованием технологии Amazon Simple Storage Service (Amazon S3).	✓	✓		✓	✓
Облачное хранение с использованием технологии IBM Cloud Object Storage.	✓	✓		✓	✓
Облачное хранение с использованием технологии IBM Cloud.	✓	✓		✓	✓
Облачное хранение с использованием технологии Microsoft Azure.	✓	✓		✓	✓
Облачное хранение с использованием технологии OpenStack Swift.	✓	✓		✓	✓
Дедупликация данных: Используйте *встроенную дедупликацию данных*, чтобы устранить дубликаты данных при записи данных в пул хранения каталога-контейнера или в пул хранения облачного контейнера. Используя встроенную дедупликацию данных, вы уменьшаете потребность в автономной реорганизации и можете повысить производительность сервера и снизить стоимость оборудования для хранения.	✓	✓	✓	✓	✓

Функция	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (с обратным порядком байт)	Microsoft Windows
Дедупликация данных: Используйте *дедупликацию данных после обработки*, чтобы устранить дубликаты данных из пулов хранения с последовательным доступом. Эта опция может привести к увеличению времени обработки, так как сервер должен распознавать данные, а затем удалять их из пула хранения.	✓	✓	✓	✓	✓
Менеджер аварийного восстановления (DRM) Подготовьте план восстановления данных сервера и клиента на случай, если произойдет авария.	✓	✓	✓	✓	✓
Встроенное сжатие данных: Данные сжимаются как при записи в пул хранения облачного контейнера или каталога контейнера, чтобы сократить объем пространства, которое занимают данные.	✓	✓	✓	✓	✓
Аутентификация Lightweight Directory Access Protocol (LDAP): Аутентифицируйте пользователей в базе данных Active Directory на сервере LDAP.	✓	✓	✓	✓	✓
Репликация узлов: Производится инкрементное копирование данных, принадлежащих узлам клиентов резервного копирования и архивирования, с одного сервера на другой.	✓	✓	✓	✓	✓
Центр операций: Производится мониторинг и управление средой хранения с использованием компонента Центр операций, пользовательского веб-интерфейса.	✓	✓	✓	✓	✓
Защита пулов хранения каталогов-контейнеров: Защищайте данные в пулах хранения каталогов-контейнеров, используя команду PROTECT STGPOOL. Можно сохранить копию данных в другом пуле хранения каталога-контейнера на целевом сервере репликации или сохранить копию на ленте в пуле хранения каталога-контейнера на том же сервере.	✓	✓ 2	✓	✓	✓
Шифрование пула хранения: Зашифруйте данные в пулах хранения облачных контейнеров.	✓	✓		✓	✓

Функция	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (с обратным порядком байт)	Microsoft Windows
Шифрование пула хранения: Зашифруйте данные в пулах хранения каталогов-контейнеров.	✓	✓	✓	✓	✓
Хранение на магнитных лентах: Сохраняйте данные на ленте, что обеспечивает гибкую и доступную возможность долгосрочного хранения данных.	✓	✓ [3]	✓	✓	✓
Протокол Transport Layer Security (TLS) 1.2: Защищенная связь с использованием TLS 1.2.	✓	✓	✓	✓	✓

[1] Технология Aspera FASP не поддерживается в Ubuntu Server LTS.

[2] Защита пулов хранения каталогов-контейнеров с записью на ленту с использованием команды PROTECT STGPOOL не поддерживается в Ubuntu Server LTS.

[3] Ленточное хранилище в системе Ubuntu Server LTS не поддерживается.

Установка и обновление сервера

Сервер IBM Spectrum Protect предоставляет клиентам услуги резервного копирования, архивирования и управления пространством. Вы можете установить или обновить один или несколько серверов в среде вашего предприятия.

- Установка сервера в системах AIX
- Установка сервера в системах Linux
- Установка сервера в системах Windows
- Обновление сервера

AIX: Установка сервера

Установка сервера включает в себя планирование, установку и первоначальное конфигурирование.

- AIX: Планирование установки сервера
  Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.
- AIX: Установка компонентов сервера
  Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.
- AIX: Первые шаги после установки IBM Spectrum Protect
  После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.
- AIX: Установка пакета исправлений сервера IBM Spectrum Protect
  Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.
- AIX: Возврат от версии 8.1.5 к предыдущему серверу
  Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.
- AIX: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect
  Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.

- AIX: Деинсталляция IBM Spectrum Protect
  Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

AIX: Планирование установки сервера

Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.

- AIX: Что нужно знать в первую очередь
  Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.
- AIX: Планирование для достижения оптимальной производительности
  Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.
-  AIX: Минимальные требования к системе для систем AIX
  Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе AIX, ознакомьтесь с требованиями к аппаратному и программному обеспечению.
-  AIX: Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе
  При определенных ограничениях на одном компьютере с сервером IBM Spectrum Protect версии 8.1.5 можно установить другие продукты, которые тоже внедряют и используют DB2.
- AIX: IBM Installation Manager
  IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.
- AIX: Контрольные списки для планирования сведений о сервере
  Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.
- AIX: Планирование мощностей
  Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.
- AIX: Практические рекомендации по именованию сервера
  Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.
- AIX: Каталоги установки
  К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

AIX: Что нужно знать в первую очередь

Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.

Выпуски пакетов сервисного обслуживания сервера, программное обеспечение клиента и публикации есть по адресу: Портал поддержки IBM®.

 Ограничение: Можно установить и запустить версию 8.1.5сервера в системе, где уже установлена DB2, причем DB2 могла быть установлена независимо или как часть другой прикладной программы, хотя существуют некоторые ограничения. Чтобы узнать об этом подробнее, смотрите раздел, посвященный совместимости с другими продуктами DB2.

Опытные администраторы DB2 смогут выполнять сложные запросы SQL и использовать инструменты DB2 для мониторинга базы данных. Однако не следует использовать инструменты DB2 ни для изменения параметров конфигурации DB2, предварительно заданных IBM Spectrum Protect, ни для модификации среды DB2 для IBM Spectrum Protect какими-либо другими способами (как это допускается при работе с другими продуктами). Сервер V8.1.5 построен и подвергнут расширенному тестированию с использованием языка определений данных (Data Definition Language - DDL) и конфигурации базы данных, которые внедряет сервер.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

AIX: Планирование для достижения оптимальной производительности

Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.

Процедура

1. Ознакомьтесь с разделом AIX: Что нужно знать в первую очередь.
2. Прочтите каждый из следующих подразделов.

- AIX: Планирование оборудования и операционной системы сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- AIX: Планирование для дисков базы данных сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- AIX: Планирование для дисков журнала восстановления сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- AIX: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров
  Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.
- AIX: Планирование для пулов хранения на устройствах классов устройств DISK или FILE
  Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.
- AIX: Планирование правильного типа технологии хранения
  У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.
- AIX: Применение наилучших практических методов к установке сервера
  Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

AIX: Планирование оборудования и операционной системы сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Соответствуют ли операционная система и оборудование требованиям или превышают их? • Число и частота процессоров • Системная память • Поддерживаемый уровень операционной системы	Если вы используете минимально необходимый объем памяти, вы можете поддерживать минимальную рабочую нагрузку. Вы можете поэкспериментировать, добавляя больше системной памяти, чтобы определить, повышается ли производительность. Затем решите, хотите ли вы оставить системную память выделенной для сервера. Проверьте различные вариации памяти, используя весь ежедневный цикл рабочей нагрузки сервера. Если у вас в системе работает несколько серверов, прибавьте требования для каждого сервера, чтобы получить требования к системе. Операционные системы AIX Ограничение: Не используйте расширение Active Memory Expansion (AME). Когда вы используете AME, программа IBM DB2 использует страницы по 4 КБ вместо страниц по 64 КБ. Каждую 4-КВ страницу нужно распаковать при получении доступа к ней, а когда она больше не будет нужна, ее следует сжать. При сжатии или распаковывании DB2 и сервер ожидают получения доступа к странице, что ухудшает производительность сервера.	Прочтите требования к операционной системе в техническом замечании 1243309. Кроме того, смотрите рекомендации в документе Задачи по настройке для операционной системы и других приложений. Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Дополнительную информацию о том, как подобрать размер для сервера и хранения, смотрите в документе IBM Spectrum Protect Blueprint.
Сконфигурированы ли диски для оптимальной производительности?	Объем настройки, которую нужно производить для разных дисковых систем, различается. Убедитесь, что задана соответствующая глубина очереди и другие опции дисковых систем.	Дополнительные сведения смотрите в следующих разделах: • "Планирование для дисков базы данных сервера" • "Планирование для дисков журнала восстановления сервера" • "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли памяти на сервере?	Для более высоких рабочих нагрузок и таких дополнительных функций, как дедупликация данных и репликация узлов, требуется объем системной памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Для баз данных, не включенных для дедупликации данных, используйте следующие рекомендации по определению требований к системной памяти: • Для баз данных, объемом менее 500 ГБ, требуется 16 ГБ памяти. • Для баз данных, объемом от 500 ГБ до 1 ТБ, требуется 24 ГБ памяти. • Для баз данных, объемом от 1 ТБ до 1,5 ТБ, требуется 32 ГБ памяти. • Для баз данных, объем которых превышает 1,5 ТБ, требуется 40 ГБ памяти. Убедитесь, что вы выделили дополнительное пространство для активного и архивного журналов для обработки репликации.	Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов • Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Есть ли в системе достаточное число адаптеров шины хоста (host bus adapter, HBA) для обработки операций с данными, которые сервер IBM Spectrum Protect должен выполнять одновременно?	Определите, для каких операций требуется использовать HBA одновременно. Например, серверу нужно сохранять 1 ГБ/сек данных резервных копий и при этом также нужно производить перенастройку пула хранения, для выполнения чего требуется 0,5 ГБ/сек. HBA должны быть способны обрабатывать все эти данные с нужной скоростью.	Смотрите раздел Настройка емкости HBA.
Превышает ли ширина полосы пропускания сети запланированную максимальную пропускную способность для резервнных копий?	Полоса пропускания сети должна позволять системе выполнять такие операции, как резервное копирование, когда это разрешено или соответствует обязательствам на уровне услуг. Для репликации узлов полоса пропускания сети должна быть больше запланированной максимальной пропускной способности.	Дополнительные сведения смотрите в следующих разделах: • Настройка производительности сети • Контрольный список по репликации узлов
Используете ли вы предпочтительную файловую систему для файлов сервера IBM Spectrum Protect?	Используйте файловую систему, обеспечивающую оптимальную производительность и доступность данных. Сервер использует прямой ввод-вывод для файловых систем, поддерживающих эту функцию. Использование прямого ввода-вывода может повысить пропускную способность и уменьшить степень использования процессора. Более подробную информацию о предпочтительной файловой системе для вашей операционной системы смотрите в документе Файловые системы, поддерживаемые сервером IBM Spectrum Protect.	Дополнительную информацию смотрите в разделе Конфигурирование операционной системы для производительности дисков.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы сконфигурировать достаточное пространство подкачки?	Пространство подкачки (или свопинга) расширяет память, доступную для обработки. Если объем свободной RAM в системе мал, программы или данные, которые не используются, перемещаются из памяти в пространство подкачки. Это действие высвобождает память для других операций, например, операций базы данных.  Операционные системы AIX Используйте, как минимум, 32 ГБ пространства подкачки или 50% оперативной памяти в зависимости от того, какое значение будет больше.	

AIX: Планирование для дисков базы данных сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Находится ли база данных на быстрых дисках с низкой латентностью?	Не используйте для базы данных IBM Spectrum Protect следующие накопители: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Не используйте внутренние диска, включенные по умолчанию в большинство аппаратных компонентов серверов. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность. Если вы собираетесь использовать функции дедупликации данных в IBM Spectrum Protect, обратите внимание на производительность дисков в виде числа операций ввода-вывода в секунду (I/O operations per second, IOPS).	Дополнительную информацию смотрите в разделе Контрольный список для дедупликации данных.
Хранится ли база данных на дисках или LUN отдельно от дисков или LUN, используемых для активного журнала, архивного журнала и томов пула хранения?	Если отделить базу данных сервера от других серверных компонентов, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно. Совет: База данных и архивный журнал могут совместно использовать массив, когда вы применяете технологию твердотельных накопителей (solid-state drive, SSD).	
Если вы используете RAID, знаете ли вы, как выбрать оптимальный уровень RAID для вашей системы? Задаете ли вы все LUN одного и того же размера и типа RAID?	Если системе нужно производить большое число операций записи, RAID 10 превосходит RAID 5. Однако для RAID 10 требуется больше дисков, чем для RAID 5 при одном и том же объеме используемого пространства хранения. Если в вашей дисковой системе используется RAID, задайте все ваши LUN с использованием одного и того же размера и типа RAID. Например, не смешивайте 4+1 RAID 5 с 4+2 RAID 6.	
Если доступна опция задать размер полосы или размер сегмента, планируете ли вы оптимизировать размер при конфигурировании дисковой системы?	Если вы можете задать размер полосы или размер сегмента, используйте в дисковых системах для базы данных размер, равный 64 КБ или 128 КБ.	Размер блока, используемого для базы данных, зависит от табличного пространства. Большинство таблиц используют блоки по 8 КБ, но некоторые используют блоки по 32 КБ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы создать хотя бы четыре каталога, которые также называются путями хранения, на четырех отдельных LUN для базы данных? Создайте по одному каталогу на отдельный массив в подсистеме. Если у вас менее трех массивов, создайте внутри массива отдельный том LUN.	При более высоких рабочих нагрузках и использовании некоторых функций требуется больше путей хранения, чем это соответствует минимальным требованиям. Такие операции сервера, как дедупликация данных, приводят к более высокому числу операций ввода-вывода в секунду (input/output operations per second, IOPS) для базы данных. Такие операции лучше выполняются, если у базы данных больше каталогов. В случае баз данных серверов, размер которых превышает 2 ТБ или которые, как ожидается, вырастут до этого размера, используйте восемь каталогов. При определении того, сколько путей хранения следует создать, рассмотрите запланированный рост системы. Сервер эффективнее использует высокое число путей хранения, если пути хранения присутствовали при первом создании сервера. Используйте переменную *DB2_PARALLEL_IO*, чтобы принудительно производить параллельный ввод-вывод в табличных пространствах, у которых один контейнер, или в табличных пространствах, контейнеры которых находятся более чем на одном физическом диске. Если вы не зададите переменную *DB2_PARALLEL_IO*, параллелизм ввода-вывода будет равен числу контейнеров, используемых табличным пространством. Например, если табличное пространство охватывает четыре контейнера, используемый уровень параллелизма ввода-вывода будет равен 4.	Дополнительные сведения смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Справку относительно того, как предсказать рост, когда сервер производит дедупликацию данных, смотрите в техническом замечании 1596944. Последнюю информацию о размере базы данных, реорганизации базы данных и замечания относительно производительности для серверов IBM Spectrum Protect смотрите в техническом замечании 1683633. Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Является ли размер всех каталогов для базы данных одинаковым?	Каталоги одного и того же размера обеспечивают одинаковую степень параллелизма для операций базы данных. Если размер одного или нескольких каталогов для базы данных меньше размера остальных каталогов, то потенциал оптимизированного предварительного извлечения снизится. Эта рекомендация также применима, если вам нужно добавить пути хранения после первоначального конфигурирования сервера.	
Собираетесь ли вы увеличить глубину очереди для LUN базы данных в системах AIX?	Глубина очереди по умолчанию часто оказывается слишком мала.	Смотрите раздел Конфигурирование систем AIX для производительности диска.

AIX: Планирование для дисков журнала восстановления сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Хранятся ли активный журнал и архивный журнал на дисках или на LUN отдельно от дисков или LUN, используемых для базы данных и томов пула хранения?	Убедитесь, что диски, на которых вы размещаете активный журнал, не используются для других задач сервера или системы. Не помещайте активный журнал на диски, содержащие базу данных сервера, архивный журнал или такие системные файлы, как пространство подкачки или свопинга.	Если отделить базу данных сервера, активный журнал и архивный журнал, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно.
Находятся ли журналы на дисках с энергонезависимым кэшем записи?	Энергонезависимый кэш записи позволяет как можно быстрее записывать данные в журналы. Более быстрые операции записи для журналов могут повысить производительность операций сервера.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задаете ли вы для журналов размер, который адекватно поддерживает рабочую нагрузку?	Если вы не уверены относительно рабочей нагрузки, используйте самый большой возможный для вас размер. Активный журнал Максимальный размер - 512 ГБ, заданный с помощью опции сервера ACTIVELOGSIZE. Убедитесь, что у вас есть хотя бы 8 ГБ свободного пространства в файловой системе активного журнала после создания активных журналов фиксированного размера. Архивный журнал Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что размер архивного журнала, как минимум, равен размеру активного журнала.	• Подробную информацию о размерах журналов смотрите в информации о журнале восстановления в техническом замечании 1421060. • Информацию о подборе размеров при использовании дедупликации данных смотрите в разделе Контрольный список для дедупликации данных.
Задаете ли вы архивный журнал передачи управления при отказе? Размещаете ли вы этот журнал на диске, являющемся отдельным по сравнению с диском архивного журнала?	Архивный журнал передачи управления при отказе предназначен для использования сервером в аварийных ситуациях, когда архивный журнал переполняется. Для архивного журнала передачи управления при отказе можно использовать более медленные диски.	Используйте опцию сервера ARCHFAILOVERLOGDIRECTORY, чтобы указать расположение архивного журнала передачи управления при отказе. Отслеживайте использование каталога для архивного журнала передачи управления при отказе. Если архивный журнал передачи управления при отказе должен использоваться сервером, пространство архивного журнала может оказаться недостаточным.
Если вы производите зеркальное отображение активного журнала, используете ли вы только один тип зеркального отображения?	Зеркальное отображение журнала можно производить, используя один из описанных ниже методов. Используйте для журнала только один тип зеркального отображения. • Используйте опцию MIRRORLOGDIRECTORY, которая доступна для сервера IBM Spectrum Protect, чтобы задать расположение зеркального отображения. • Используйте в AIX зеркальное отображение программ, например, Logical Volume Manager (LVM). • Используйте зеркальное отображение на оборудовании дисковых систем.	Если вы зеркально отображаете активный журнал, убедитесь, что у дисков для активного журнала и зеркальной копии одинаковая скорость и надежность. Дополнительную информацию смотрите в разделе Конфигурирование и настройка журнала восстановления.

AIX: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров

Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы быстрое дисковое хранения для базы данных IBM Spectrum Protect, если измерять ее в операциях ввода-вывода в секунду (input/output operations per second, IOPS)?	Используйте для базы данных высокопроизводительный диск. Используйте технологию твердотельных дисков для обработки дедупликации данных. Убедитесь, что база данных обеспечивает минимальное значение в 3000 IOPS. Для каждого терабайта данных, копируемого в день (до дедупликации данных) прибавьте к этому минимуму 1000 IOPS. Например, для сервера IBM Spectrum Protect, который пропускает 3 ТБ данных в день, потребуется 6000 IOPS для дисков базы данных: `минимум 3000 IOPS + 3000 (3 ТБ x 1000 IOPS) = 6000 IOPS`	Рекомендации относительно выбора диска смотрите в разделе "Планирование для дисков базы данных сервера". Дополнительные сведения об IOPS смотрите в документах IBM Spectrum Protect Макеты.
Достаточно ли памяти для размера вашей базы данных?	Для серверов IBM Spectrum Protect с размером базы данных, равным 100 ГБ, которые производят дедупликацию данных, используйте, как минимум, 40 ГБ системной памяти. Если сохраняемый объем данных резервных копий возрастает, может понадобиться увеличить требования к системной памяти. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память. Используйте больше памяти, чтобы улучшить кэширование страниц базы данных. Приведенные ниже рекомендация по размеру памяти основаны на ежедневном объеме новых данных, резервные копии которых вы создаете: • 128 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 1-2 ТБ • 192 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 2-4 ТБ	Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Правильно ли вы подобрали размер емкости хранения для активного и архивного журналов базы данных?	Сконфигурируйте для сервера минимальный размер активного журнала 128 Гбайт, задав для опции сервера ACTIVELOGSIZE значение 131072. Рекомендуемый начальный размер архивного журнала - 1 ТБ. Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что для файловой системы есть хотя бы 10% дополнительного пространства на диске, превышающего размер архивного журнала. Используйте для архивных журналов баз данных каталог с начальной свободной емкостью, как минимум, 1 ТБ. Задайте каталог при помощи опции сервера ARCHLOGDIRECTORY. Определите пространство для архивного журнала восстановления после отказа при помощи опции сервера ARCHFAILOVERLOGDIRECTORY.	Дополнительную информацию о том, как подобрать размер системы, смотрите в документах IBM Spectrum Protect Макеты.
Включено ли сжатие для архивного журнала и резервных копий базы данных?	Включите опцию сервера ARCHLOGCOMPRESS, чтобы сэкономить пространство хранения. Эта опция сжатия отличается от строенного сжатия. Встроенное сжатие по умолчанию включено в IBM Spectrum Protect V7.1.5 и новее. Ограничение: Не используйте эту опцию, если объем резервных копий данных превышает 6 ТБ в день.	Дополнительную информацию о сжатии для вашей системы смотрите в документах IBM Spectrum Protect Макеты.
Расположены ли база данных и журналы IBM Spectrum Protect в разных томах диска (LUN)? Сконфигурирован ли диск, который используется для базы данных, в соответствии с рекомендациями для транзакционной базы данных?	База данных не должна использовать дисковые тома совместно с журналами или пулами хранения IBM Spectrum Protect, с другим приложением или с другой файловой системой.	Дополнительную информацию о базе данных сервера и конфигурации журнала восстановления смотрите в документе Конфигурирование и настройка базы данных сервера и журнала восстановления.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы, как минимум, восемь (2,2 ГГц или эквивалент) ядер процессора для каждого сервера IBM Spectrum Protect, который вы хотите использовать в сочетании с дедупликацией данных?	Если планируется использование дедупликации данных на стороне клиента, проверьте, есть ли у систем клиентов адекватные ресурсы, доступные во время операции резервного копирования, чтобы выполнять обработку дедупликации данных. Используйте процессор, эквивалентный по крайней мере одному процессорному ядру 2,2 ГГц, на каждый процесс резервного копирования с дедупликацией данных на стороне клиента.	• Эффективное планирование и использование дедупликации • IBM Spectrum Protect Макеты
Выделен ли вами достаточный объем пространства хранения для базы данных?	В первом приближении нужно запланировать выделение 100 ГБ для хранения базы данных на каждые 50 ТБ данных, которые будут защищены в дедуплицированных пулах хранения. *Защищенные данные* - это объем данных перед дедупликацией данных, включая все версии сохраненных объектов. Лучше всего задать новый пул хранения исключительно для дедупликации данных. Дедупликация данных производится на уровне пула хранения. Дедупликации подвергаются все данные, содержащиеся в пуле хранения, за исключением зашифрованных данных.	
Оценили ли вы емкость пула хранения для конфигурирования достаточного пространства, соответствующего размеру вашей среды?	Для оценки требований к емкости для дедуплицированного пула хранения можно использовать следующий метод: 1. Оцените базовый размер данных источника. 2. Оцените ежедневный размер резервных копий, используя предполагаемый темп изменений и роста. 3. Определите требования к сроку хранения. 4. Вычислите общий размер данных данных источника с учетом базового размера, ежедневного размера резервных копий и требований к сроку хранения. 5. Примените коэффициент дедупликации. 6. Примените коэффициент сжатия. 7. Округлите оценку, чтобы учесть переходное использование пула хранения.	Пример использования этого метода смотрите на веб-странице Эффективное планирование и использование дедупликации.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Распределили ли вы операции дискового ввода-вывода по нескольким дисковым устройствам и контроллерам?	Используйте массивы, которые состоят из как можно большего количества дисков (иногда это называется 'широкое чередование'. Убедитесь, что вы используете один каталог базы данных для отдельного массива в подсистеме. Задайте переменную реестра *DB2_PARALLEL_IO*, так чтобы включить параллельный ввод-вывод для каждого табличного пространства, используемого, если контейнеры в табличном пространстве охватывают несколько физических дисков. Если полоса пропускания для ввода-вывода доступна, а размер файлов велик (например, 1 МБ), процесс нахождения дубликатов может использовать ресурсы всего процессора. Когда файлы меньше, более критичны другие узкие места. Задайте восемь или больше файловых систем для класса устройств дедуплицированного пула хранения, чтобы операции ввода-вывода распределялись по максимально возможному числу LUN и физических устройств.	Рекомендации по настройке пулов хранения смотрите в разделе "Планирование для пулов хранения на устройствах классов устройств DISK или FILE". Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.
Запланировали ли вы ежедневные операции на основе вашей стратегии резервного копирования?	Наилучшая последовательность операций будет следующей: 1. Резервное копирование клиента 2. Защита пула хранения 3. Репликация узлов 4. Резервное копирование базы данных 5. Окончание действия устаревших файлов	• Планирование дедупликации данных и процессов репликации узла • Ежедневные операции для пулов хранения каталогов-контейнеров

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли у вас пространства хранения для управления списком блокировки DB2?	Если выполняется дедупликация данных, в состав которых входят большие объекты или большое число одновременно обрабатываемых файлов, процесс может привести к тому, что станет не хватать пространства хранения. При нехватке пространства хранения списка блокировок могут происходить ошибки резервного копирования, отказы процессов управления данными или перерывы в работе сервера. Если дедупликация данных обрабатывает файлы размером более 500 ГБ, это вероятнее всего приведет к истощению пространства хранения. Но если большое число выполняемых операций резервного копирования использует дедупликацию данных на стороне клиента, эта проблема может также произойти и с файлами меньшего размера.	Информацию о настройке параметра DB2 LOCKLIST смотрите в документе Настройка дедупликации данных на стороне сервера.
Доступна ли достаточная полоса пропускания для передачи данных на сервер IBM Spectrum Protect?	Чтобы переносить данные на сервер IBM Spectrum Protect, используйте дедупликацию данных на стороне клиента или на стороне сервера и сжатие, чтобы уменьшить необходимую ширину полосы пропускания. Используйте сервер V7.1.5 или новее, чтобы применить встроенное сжатие, и используйте клиент V7.1.6 или новее, чтобы включить усовершенствованную обработку сжатия.	Дополнительные сведения смотрите в описании опции клиента enablededup.
Определили ли вы, сколько каталогов пула хранения следует назначить для каждого пула хранения?	Назначьте каталоги для пула хранения, используя команду DEFINE STGPOOLDIRECTORY. Создайте несколько каталогов пула хранения и убедитесь, что для каждого каталога создается резервная копия на отдельном дисковом томе (LUN).	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Выделен ли вами достаточный объем дискового пространства в пуле хранения облачных контейнеров?	Чтобы предотвратить ошибки резервного копирования, убедитесь, что в локальном каталоге достаточно места. Оптимальный размер дискового пространства указан ниже в списке: • Для SCSI с последовательным подключением (SAS) и вращающегося диска вычислите объем новых данных, ожидаемых поле ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства. • Для систем хранения на основе флэш-памяти, у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 3 Тбайт. • Для систем хранения с твердотельными накопителями (SSD), у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 5 Тбайт.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Выбрали ли вы подходящий тип локальной системы хранения?	Убедитесь, что передача данных из локальной системы хранения в облако завершена до начала следующего цикла резервного копирования.
	Совет: Данные удаляются из локальной системы хранения вскоре после их перемещения в облако.
	Учтите следующие рекомендации:
	• Используйте флеш-память или твердотельные накопители (SSD) для больших облачных система высокой производительности. Убедитесь, что у вас есть ссылка на глобальную сеть (wide area network, WAN) с выделенными 10 Гбайт памяти и высокоскоростным соединением с хранилищем объектов. Например, используйте флеш-память или SSD, если у вас выделенная ссылка 10 ГБ WAN плюс высокоскоростное соединение либо с расположением IBM® Cloud Object Storage, либо с центром данных Amazon Simple Storage Service (Amazon S3).
	• Для указанных ниже сценариев используйте диски SAS большей емкости 15000 rpm:
	  ○ Системы среднего размера
	  ○ Медленные соединения с облаком, например 1 Гбайт
	  ○ При использовании IBM Cloud Object Storage в качестве провайдера службы в нескольких регионах
	• Для SAS или вращающегося диска вычислите объем новых данных, ожидаемых после ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства.	

AIX: Планирование для пулов хранения на устройствах классов устройств DISK или FILE

Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Могут ли LUN пула хранения поддерживать пропускную способность для последовательного чтения и записи, объемом 256 КБ, чтобы адекватно обрабатывать рабочую нагрузку в пределах ограничений времени?	При планировании пиковых нагрузок учитывайте все данные, которые сервер должен читать из дисковых пулов хранения или записывать в дисковые пулы хранения одновременно. Например, рассмотрим пиковый поток данных от одновременно выполняющихся операций резервного копирования клиента и операций по перемещению данных сервером, например, перенастройку. В подавляющем большинстве случаев сервер IBM Spectrum Protect производит чтение из пулов хранения и записывает данные в пулы хранения блоками по 156 КБ. Если дисковая система обеспечивает такую возможность, сконфигурируйте дисковую систему для оптимальной производительности при выполнении последовательных операций чтения/записи, а не случайных операций чтения/записи.	Дополнительную информацию смотрите в документе Анализ базовой производительности дисковых систем.
Сконфигурирован ли диск для использования кэша чтения и записи?	Используйте больший объем кэша, чтобы повысить производительность.	
Определили ли вы правильный размер, который следует использовать для томов пула хранения, когда пулы хранения используют класс устройств FILE?	Ознакомьтесь с информацией в разделе Оптимальное число и размер томов для пулов хранения, использующих диск. Если у вас нет информации, которая бы позволила оценить размер томов класса устройств FILE, начните с томов, имеющих 50 ГБ.	Как правило, проблемы чаще возникают, если тома слишком малы. Если тома больше, чем требуется, сообщается о малом числе проблем. Когда вы определите размер тома, который следует использовать, в качестве предосторожности выберите размер, который может оказаться больше необходимого.
Используете ли вы заранее выделенные тома для пулов хранения, использующих классы устройств FILE?	Чистые тома могут вызвать фрагментацию файлов. Чтобы убедиться, что пулу хранения будет хватать томов, задайте для параметра MAXSCRATCH значение больше нуля.	Используйте серверную команду DEFINE VOLUME, чтобы заранее выделить тома в пуле хранения. Используйте серверную команду DEFINE STGPOOL или UPDATE STGPOOL, чтобы задать параметр MAXSCRATCH.
Сравнивали ли вы максимальное число сеансов клиентов с числом заданных томов для пулов хранения, использующих классы устройств FILE?	Всегда оставляйте в пулах хранения достаточное число пригодных для использования томов, чтобы разрешить одновременное выполнение ожидаемого пикового числа сеансов клиентов. Тома могут быть чистыми, пустыми или частично заполненными томами.	В случае пулов хранения, которые используют класс устройств FILE, на том одновременно может производить запись только один сеанс или процесс.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задали ли вы для параметра MOUNTLIMIT класса устройств достаточно высокое значение, чтобы учесть число томов, которые могут быть смонтированы параллельно, когда пулы хранения используют класс устройств FILE?	Для пулов хранения, использующих дедупликацию данных, параметр MOUNTLIMIT, как правило, находится в диапазоне 500-1000. Задайте для MOUNTLIMIT значение, равное максимальному числу необходимых точек монтирования, необходимых для всех активных сеансов. Рассмотрим параметры, которые влияют на максимальное число необходимых точек монтирования: • Опция сервера MAXSESSIONS, представляющая собой максимальное число сеансов IBM Spectrum Protect, которые могут выполняться одновременно. • Параметр MAXNUMMP, указывающий, какое максимальное число точек монтирования может использовать каждый клиентский узел. Например, если максимальное число сеансов резервного копирования клиентских узлов, как правило, составляет 100, а для каждого из узлов задан параметр `MAXNUMMP=2`, умножьте 100 узлов на 2 точки монтирования для каждого узла, чтобы получить значение 200 для параметра MOUNTLIMIT.	Используя серверную команду REGISTER NODE или UPDATE NODE, задайте параметр MAXNUMMP для клиентских узлов.
Определили ли вы, сколько томов пула хранения поместить в каждую файловую систему для пулов хранения, использующих классы устройств DISK?	То, как вы конфигурируете пространство хранения для пула хранения, использующего класс устройств DISK, зависит от того, используете ли вы RAID для дисковой системы. Если вы не используете RAID, сконфигурируйте по одной файловой системе на физический диск и задайте по одному тому пула хранения для каждой файловой системы. Если вы используете RAID 5 с *n*+1 томами, сконфигурируйте пространство хранения одним из следующих способов: • Сконфигурируйте *n* файловых систем на LUN и задайте по одному тому пула хранения для файловой системы. • Сконфигурируйте одну файловую систему и *n* томов пула хранения для LUN.	Пример схемы, соответствующей этой рекомендации, смотрите в документе Пример схемы пулов хранения сервера.
Создали ли вы пулы хранения для распределения операций ввода-вывода по нескольким файловым системам?	Убедитесь, что каждая файловая система находится на отдельном LUN в дисковой системе. Как правило, 10-30 файловых систем - это оптимальная цель, но вы должны убедиться, что размер файловых систем будет не менее, чем 250 ГБ (примерно).	Дополнительные сведения смотрите в следующих разделах: • Настройка дискового хранения для сервера • Настройка и конфигурирование пулов хранения и томов

AIX: Планирование правильного типа технологии хранения

У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.

Процедура

Ознакомьтесь со следующей таблицей, которая поможет вам выбрать правильный тип технологии хранения для ресурсов хранения, необходимых серверу.

Табл. 1. Типы технологии хранения в требованиях по хранению IBM Spectrum Protect

Тип технологии хранения	**Database**	**Активный журнал**	**Архивный журнал и резервный архивный журнал**	**Пулы хранения**
Твердотельный диск (Solid-state disk, SSD)	Размещайте базу данных на SSD при следующих обстоятельствах: • Вы используете дедупликацию данных IBM Spectrum Protect. • Вы ежедневно производите резервное копирование более чем 8 ТБ новых данных.	Если вы поместите базу данных IBM Spectrum Protect на SSD, лучше всего поместить активный журнал на SSD. Если пространство недоступно, используйте вместо этого высокопроизводит. диск.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Архивный журнал и архивные журналы передачи управления при отказе можно поместить на носители с более медленными типами технологии хранения.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Пулы хранения можно поместить на носители с более медленными типами технологии хранения.
Высокопроизв. диск со следующими хар-ками: • **Диск 15 К rpm** • **Оптоволокно (Fibre Channel) интерфейс или последов. подкл. интерфейс SCSI (SAS).**	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Высокопроизв. диски можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте высокопроизв. диски для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.

Тип технологии хранения	Database	Активный журнал	Архивный журнал и резервный архивный журнал	Пулы хранения
Диск средней произв. или высокопроизв. диск со следующими хар-ками: • **Диск 10 K rpm** • **Оптоволокно (Fibre Channel) интерфейс или интерфейс SAS**	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Диск средней производительности или высокопроизв. диск можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте диск средней производительности или высокопроизв. диск для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.
SATA, пространство хранения, подключенное к сети	Не используйте этот тип хранения для базы данных. Не помещайте базу данных в системы хранения XIV.	Не используйте этот тип хранения для активного журнала.	Использование этой более медленной технологии хранения является приемлемым, так как эти журналы записываются один раз и редко читаются.	Используйте эту более медленную технологию хранения при следующих обстоятельствах: • Данные редко записываются, например, записываются один раз. • Данные редко читаются. .
Лента и виртуальная лента				Используйте для долгосрочного хранения, если данные используются нечасто.

AIX: Применение наилучших практических методов к установке сервера

Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Процедура

- Описанные ниже наилучшие методы являются наиболее важными для достижения оптимальной производительности и предотвращения ошибок.
- Смотрите таблицу, чтобы определить наилучшие методы, применимые к вашей среде.

Практическая рекомендация	Дополнительная информация
Используйте для базы данных сервера быстрые диски. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность.	Используйте для базы данных быстрые диски с низкой латентностью. Использование SSD является существенным, если вы используете дедупликацию данных и репликацию узлов. Старайтесь не использовать диски Serial Advanced Technology Attachment (SATA) и Parallel Advanced Technology Attachment (PATA). Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование правильного типа технологии хранения"
Убедитесь, что в системе сервера достаточно памяти.	Прочтите требования к операционной системе в техническом замечании 1243309. При более высоких рабочих нагрузках требуется больше ресурсов, чем указано в минимальных требованиях. Такие дополнительные функции, как дедупликация данных и репликация узлов, могут потребовать объем памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Если вы планируете запускать несколько экземпляров сервера, каждому экземпляру потребуется объем памяти, указанный для одного сервера. Умножьте объем памяти для одного сервера на число экземпляров, которые вы собираетесь запускать в системе.
Отделите базу данных сервера, активный журнал, архивный журнал и дисковые пулы хранения друг от друга.	Держите все ресурсы хранения IBM Spectrum Protect на отдельных дисках. Держите диски пулов хранения храниться отдельно от дисков базы данных сервера и журналов. Операции пулов хранения могут перекрываться операциями базы данных, если они находятся на одних и тех же дисках. В идеале база данных сервера и журналы также должны быть отделены друг от друга. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование для дисков журнала восстановления сервера" ○ "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"
Используйте для базы данных сервера хотя бы четыре каталога. Для больших серверов или серверов, использующих дополнительные функции, используйте восемь каталогов.	Поместите каждый каталог на LUN, изолированный от других LUN и от других приложений. Сервер считается большим, если его база данных превышает 2 ТБ или если ожидается, что она вырастет больше этого размера. Используйте для таких серверов восемь каталогов. Смотрите раздел "Планирование для дисков базы данных сервера".
Если вы используете дедупликацию данных и/или репликацию узлов, следуйте рекомендациям по конфигурированию базы данных и других элементов.	Сконфигурируйте базу данных сервера в соответствии с рекомендациями, так как база данных чрезвычайно важна для того, чтобы сервер смог хорошо работать, если используются такие функции. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ Контрольный список для дедупликации данных ○ Контрольный список по репликации узлов

Практическая рекомендация	Дополнительная информация
В случае пулов хранения, которые используют класс устройств типа FILE, выполните рекомендации по размеру томов пула хранения. Как правило, тома 50 ГБ подходят лучше всего.	Прочтите информацию в разделе Оптимальное число и размер томов для пулов хранения, использующих диск, чтобы это помогло вам определить размер тома. Сконфигурируйте устройства пула хранения и файловые системы на основе требований к пропускной способности, а не только на основе требований к емкости. Изолируйте устройства хранения, используемые продуктом IBM Spectrum Protect, от других приложений с высоким объемом ввода-вывода и убедитесь, что для этого хранилища обеспечивается достаточная пропускная способность. Дополнительные сведения смотрите в разделе Контрольный список для пулов хранения на устройствах DISK или FILE.
Запланируйте операции клиента IBM Spectrum Protect и действия по обслуживанию сервера, чтобы избежать перекрывания операций или свести такое перекрывание к минимуму.	Дополнительные сведения смотрите в следующих разделах: ◦ Настройка расписания для ежедневных операций ◦ Контрольный список для конфигурации сервера
Постоянно осуществляйте мониторинг операций.	Проводя мониторинг, вы сможете раньше находить ошибки и вам будет проще выявлять их причины. Срок хранения записей отчетов мониторинга может доходить до года - это поможет вам выявлять тенденции и планировать рост. Смотрите раздел Мониторинг среды и ее обслуживание с целью обеспечения производительности.

AIX: Минимальные требования к системе для систем AIX

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе AIX, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Оптимальная среда IBM Spectrum Protect настраивается с дедупликацией данных с использованием IBM Spectrum Protect Blueprints.

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

 Операционные системы AIX

AIX: Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе

При определенных ограничениях на одном компьютере с сервером IBM Spectrum Protect версии 8.1.5 можно установить другие продукты, которые тоже внедряют и используют DB2.

Если вы хотите установить и использовать другие продукты, которые используют продукт DB2, на одном компьютере с сервером IBM Spectrum Protect, убедитесь, что выполняются следующие условия:

Табл. 1. Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе

Критерий	Инструкции
Уровень версии	Другие продукты, использующие DB2, должны использовать DB2 версии 9 или новее. Продукты DB2 включают в себя поддержку инкапсуляции и разделения продуктов, начиная с версии 9. Начиная с этой версии, можно запускать несколько копий продуктов DB2 с разными уровнями кода в одной системе. Чтобы узнать об этом подробнее, смотрите информацию о нескольких копиях DB2 по адресу: Информация о DB2.
ID и каталоги пользователей	Убедитесь, что ID пользователей, ID изолированных пользователей, положение установки, другие каталоги и связанная информация не используются одновременно в нескольких установках DB2. Ваши спецификации должны отличаться от тех ID и положений, которые использовались для установки и конфигурирования сервера IBM Spectrum Protect. Если вы сконфигурировали сервер при помощи мастера dsmicfgx, это будут значения, введенные вами во время работы с мастером. Если вы использовали метод конфигурирования вручную, вспомните, какие значения вы использовали для сервера при выполнении этих процедур (если это потребуется).
Выделение ресурсов	Оцените ресурсы и возможности системы, сопоставив их как с требованиями для сервера IBM Spectrum Protect, так и для других программ, которые используют продукт DB2. Чтобы обеспечить достаточно ресурсов для других приложений DB2, нужно изменить параметры сервера IBM Spectrum Protect, так чтобы сервер использовал меньше памяти и ресурсов. Аналогичным образом, если рабочие нагрузки для других приложений DB2 таковы, что между этими приложениями и сервером IBM Spectrum Protect возникает конфликт доступа к ресурсам процессора или памяти, это может отрицательно сказаться на производительности сервера при обработке ожидаемой рабочей нагрузке клиента или при выполнении других серверных операций. Чтобы разделить ресурсы и обеспечить больше возможностей настройки и распределения ресурсов процессора и памяти и других системных ресурсов между несколькими приложениями, рассмотрите возможность использования логических разделов (Logical Partition - LPAR), разделов рабочей нагрузки (Workload Partition - WPAR) или иной поддержки виртуальных рабочих станций. Например, запускайте программу DB2 в ее собственной виртуальной системе.

AIX: IBM Installation Manager

IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке IBM Spectrum Protect. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать IBM Spectrum Protect.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение
: Устанавливаемый модуль программного продукта.

  Предложение IBM Spectrum Protect содержит все носители, которые требуются IBM Installation Manager для установки IBM Spectrum Protect.

Пакет
: Группа программных компонентов, необходимых для установки предложения.
  Пакет IBM Spectrum Protect включает в себя следующие компоненты:

  - Программа установки IBM Installation Manager
  - Предложение IBM Spectrum Protect

Группа пакетов
: Набор пакетов, использующих общий родительский каталог.

  Группа пакетов по умолчанию для пакета IBM Spectrum Protect - `IBM Installation Manager`.

Репозиторий
: Удаленная или локальная область хранения данных и других ресурсов программы.

  Пакет IBM Spectrum Protect хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
: Каталог, содержащий файлы или подключаемые модули программ, которые совместно используются пакетами.

  IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии IBM Spectrum Protect.

AIX: Контрольные списки для планирования сведений о сервере

Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.

Элемент	Необходимое пространство	Число каталогов	Положение каталогов
База данных			
Активный журнал			
Архивный журнал			
Необязательно: Зеркальная копия активного журнала			
Необязательно: Вторичный архивный журнал (резервный каталог для архивного журнала)			

Элемент	Имена и ID пользователей	Расположение
ID пользователя экземпляра для сервера, то есть ID, который использовался для запуска и работы сервера IBM Spectrum Protect		
Домашний каталог для сервера, то есть каталог, содержащий ID пользователя экземпляра		
Имя экземпляра базы данных		
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)		
Имя сервера; для каждого сервера используйте уникальное имя		

AIX: Планирование мощностей

Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части

планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.

- AIX: Оценка необходимого объема пространства для базы данных
  Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.
- AIX: Требования к пространству журнала восстановления
  В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.
- AIX: Мониторинг использования пространства для базы данных и журналов восстановления
  Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.
- AIX: Удаление файлов отката установки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

AIX: Оценка необходимого объема пространства для базы данных

Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.

Об этой задаче

В качестве начального объема пространства базы данных можно порекомендовать использовать не менее 25 ГБ. Доступ к пространству файловой системы предоставляется должным образом. Размер базы данных 25 ГБ достаточен для среды тестирования или среды, включающей только менеджер библиотек. Для производственного сервера с поддержкой клиентских рабочих нагрузок размер базы данных должен быть больше. Если вы используете дисковые пулы хранения с произвольным доступом (DISK), потребуется дополнительное пространство хранения баз данных и журналов для пулов хранения с последовательным доступом.

Максимальный размер базы данных IBM Spectrum Protect - 6 ТБ.

Информацию об оценке размера базы данных в производственной среде на основе числа файлов и размера пула хранения смотрите в темах ниже.

- AIX: Оценка требований к пространству базы данных на основе числа файлов
  Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.
- AIX: Оценка требований к пространству базы данных на основе мощности пула хранения
  Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.
- AIX: Менеджер баз данных и временное пространство
  Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

AIX: Оценка требований к пространству базы данных на основе числа файлов

Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.

Об этой задаче

Для оценки требований к объему пространства на основе максимального числа файлов в системе хранения сервера используйте следующие рекомендации:

- 600 - 1000 байт на каждую хранимую версию файла, включая резервные копии образов.
  Ограничение: Сюда не входит пространство, используемое во время дедупликации данных.
- 100 - 200 байт на каждый кэшированный файл, файл пула хранения копий, файл пула активных данных и дедуплицированный файл.
- Дополнительное пространство требуется для оптимизации базы данных в части поддержки переменных схем доступа к данным и внутренней обработки данных на сервере. Объем дополнительного пространства равен 50% оцененного размера памяти для хранения файловых объектов.

В следующем примере для единственного клиента вычисления основываются на максимальных значениях из предыдущих инструкций. В примерах не учитывается возможное использование объединения файлов. В общем случае объединение файлов сокращает объем требуемого пространства базы данных. Объединение файлов не затрагивает перенесенные файлы.

Процедура

1. Вычислите число версий файлов. Чтобы получить число версий файлов, сложите следующие значения:
   a. Вычислите число резервных копий файлов. Например, одновременно может существовать до 500 000 резервных копий клиентских файлов. В этом примере политики хранения требуют, чтобы хранилось до трех резервных копий каждого файла:

      ```
      500 000 файлов * 3 копии = 1 500 000 файлов
      ```

   b. Вычислите количество архивных файлов. Например, до 100 000 клиентских файлов могут быть архивными копиями.
   c. Вычислите количество перенесенных файлов. Например, до 200 000 клиентских файлов могут быть перемещены с клиентских рабочих станций.

   Если для каждого файла требуется 1000 байт, то общий объем требуемого для принадлежащих клиентам файлов пространства базы данных - 1,8 ГБ.

   ```
   (1 500 000 + 100 000 + 200 000) * 1000 = 1,8 ГБ
   ```

2. Вычислите число кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов:
   a. Вычислите количество кэшированных копий. Например, кэширование разрешено в дисковом пуле хранения размером 5 ГБ. Верхний порог переноса пула равен 90%, а нижний - 70%. Таким образом, 20% дискового пула, то есть 1 ГБ, будет занято кэшированными файлами.
   Если средний размер файла около 10 КБ, в кэше в любой момент времени находится около 100000 файлов:

      ```
      100 000 файлов * 200
      байт = 19 МБ
      ```

   b. Вычислите количество файлов пула хранения копий. Для всех основных пулов памяти создается резервная копия:

      ```
      (1 500 000 + 100 000 + 200 000) * 200 байт = 343 МБ
      ```

   c. Вычислите количество активных файлов пула хранения. Все данные активных резервных копий клиента в первичных пулах хранения копируются в пул хранения активных данных. Допустим, что 500 000 версий 1 500 000 резервных копий файлов в основном пуле являются активными:

      ```
      500 000 * 200 байт = 95 МБ
      ```

   d. Вычислите количество дедуплицированных данных. Допустим, что пул хранения данных, подвергнутых дедупликации, содержит 50000 файлов:

      ```
      50 000 * 200 байт = 10 МБ
      ```

   На основании этих вычислений для клиентских кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов требуется примерно 0,5 ГБ дополнительного пространства базы данных.

3. Вычислите объем дополнительного пространства, требуемый для оптимизации базы данных. Для обеспечения оптимального доступа к данным и управления сервером требуется дополнительное пространство базы данных. Объем дополнительного пространства базы данных равен 50% общего пространства, необходимого для хранения файловых объектов.

   ```
   (1,8 + 0,5) * 50% = 1,2 ГБ
   ```

4. Вычислите общий объем пространства базы данных, требуемый для этого клиента. Общий объем составит примерно 3,5 ГБ:

   ```
   1,8 + 0,5 + 1,2 = 3,5 ГБ
   ```

5. Вычислите общий объем пространства базы данных, требуемый для всех клиентов. Если предыдущие оценки приведены для типичного клиента и у вас 500 таких клиентов, то можно использовать для примера следующую оценку общего объема пространства базы данных, требуемого для всех клиентов:

   ```
   500 * 3,5 = 1,7 ТБ
   ```

Результаты

Совет: В приведенных выше примерах результаты представляют собой примерные оценки. Фактический размер базы данных может отличаться от ожидаемого из-за таких факторов, как число каталогов и длина полных имен файлов. Рекомендуется периодически производить мониторинг базы данных и корректировать ее размер, если потребуется.

Дальнейшие действия

При обычных операциях серверу IBM Spectrum Protect может потребоваться временное пространство баз данных. Это пространство необходимо для следующих задач:

- Сохранять результаты сортировки или упорядочивания, которые еще не сохранены и не оптимизированы непосредственно в базе данных. Эти результаты временно сохраняются в базе данных для обработки.
- Предоставлять административный доступ к базе данных одним из следующих способов:
  - Через клиент Open Database Connectivity (ODBC) DB2
  - Через клиент Oracle Java™ Database Connectivity (JDBC)
  - Из командной строки клиента администрирования на сервер с помощью Structured Query Language (SQL)

Используйте дополнительные 50 ГБ временного пространства на каждые 500 ГБ пространства для файловых объектов и оптимизации. Смотрите инструкции в следующей таблице. В примере, использованном в предыдущем шаге, для файловых объектов и оптимизации для 500 клиентов требуется общий объем пространства базы данных 1,7 ТБ. На основании этих оценок еще около 200 ГБ требуется для временного пространства. Суммарный объем требуемого пространства базы данных составляет 1,9 ТБ.

Размер базы данных	Минимальные потребности временного пространства
< 500 ГБ	50 ГБ
≥ 500 ГБ и < 1 ТБ	100 ГБ
≥ 1 ТБ и < 1,5 ТБ	150 ГБ
≥ 1,5 и < 2 ТБ	200 ГБ
≥ 2 и < 3 ТБ	250 - 300 ГБ
≥ 3 и < 4 ТБ	350 - 400 ГБ

AIX: Оценка требований к пространству базы данных на основе мощности пула хранения

Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.

AIX: Менеджер баз данных и временное пространство

Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Менеджер баз данных сортирует данные в определенном порядке, как в операторе SQL, который вводится для запроса данных. В зависимости от рабочей нагрузки на сервере, если объем данных больше, чем может обрабатывать менеджер баз данных, эти упорядоченные данные размещаются во временном дисковом пространстве. Данные располагаются во временном дисковом пространстве, когда уже существует большой набор результатов. Менеджер баз данных динамически управляет памятью, используемой при размещении данных во временном дисковом пространстве.

Например, большой объем результатов может возникнуть при обработке устаревания данных. Если памяти системы недостаточно для хранения набора результатов, некоторые данные размещаются во временной дисковом пространстве. Если во время обработки устаревания выбран чрезмерно большой узел или файловое пространство, то менеджер баз данных не сможет отсортировать данные в памяти. Для сортировки данных менеджеру баз данных понадобится временное пространство.

Чтобы запустить операции базы данных, рассмотрите возможность добавления пространства базы данных для следующих сценариев:

- У базы данных маленький объем пространства, и операции сервера, которым требуется временное пространство, используют оставшуюся незанятую память.
- Файловые пространства велики, или для них назначена политика, которая создает много версий файлов.
- Сервер IBM Spectrum Protect должен быть запущен с ограниченным объемом памяти. Для запуска своих операций база данных использует главную память сервера IBM Spectrum Protect. Однако если памяти недостаточно, сервер IBM Spectrum Protect выделяет для базы данных временное пространство на диске. Например, если доступно 10 ГБ памяти, а для операций базы данных требуется 12 ГБ, база данных использует временное пространство.
- При внедрении сервера IBM Spectrum Protect появится сообщение об ошибке `недостаток памяти базы данных`. Отслеживайте в активном журнале сервера сообщения, относящиеся к пространству баз данных.

Важное замечание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами Fix Pack IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, чтобы не повредить базу данных.

AIX: Требования к пространству журнала восстановления

В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.

- AIX: Пространство активных и архивных журналов
  Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.
- AIX: Пространство зеркальной копии активного журнала
  Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.
- AIX: Пространство резервного архивного журнала
  Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

AIX: Пространство активных и архивных журналов

Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.

Максимальный размер активного журнала для серверов IBM Spectrum Protect версии 7.1 и новее должен составлять 512 ГБ. Размер архивного журнала ограничен размером файловой системы, в которой он установлен.

Учитывайте следующие общие рекомендации для оценки размера активного журнала:

- Рекомендуемый начальный размер активного журнала - 16 Гбайт.
- Убедитесь, что размер активного журнала достаточен, по крайней мере, для тех текущих операций, которые обычно обрабатываются сервером. В качестве меры предосторожности попытайтесь учесть наибольший объем работы, которую сервер может выполнять единовременно. Обеспечьте для активного журнала некоторый дополнительный объем пространства, которое может использоваться при необходимости. Предусмотрите 20% дополнительного пространства.
- Отслеживайте используемое и доступное пространство активного журнала. При необходимости подстраивайте размер активного журнала в зависимости от таких факторов, как активность клиентов и уровень операций сервера.
- Убедитесь, что размер каталога, в котором содержится активный журнал, не меньше размера самого журнала. Если каталог больше по размеру, чем активный журнал, при необходимости он может использоваться для обработки аварийного восстановления.
- Убедитесь, что в файловой системе, которая содержит каталог активного журнала, есть по крайней мере 8 Гбайт свободного места для требований временных перемещений журналов.

Рекомендуемый начальный размер архивного журнала - 48 Гбайт.

Каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала, сгенерированные с момента последнего полного резервного копирования. Например, если вы производите резервное копирование базы данных ежедневно, каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала для всех операций клиентов в течение 24 часов. Чтобы освободить пространство, при полном резервном копировании базы данных сервер удаляет устаревшие файлы архивного журнала. Если каталог архивного журнала переполняется, а каталог резервного архивного журнала не существует, файлы журнала остаются в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением каталога активного журнала. При повторном запуске сервера часть используемого для активного журнала пространства освобождается.

После установки сервера вы можете отслеживать использование архивного журнала и пространство каталога архивного журнала. Если каталог архивного журнала переполняется, то это может привести к следующим проблемам:

- Сервер не сможет провести полное резервное копирование базы данных. Исследуйте и разрешите эту проблему.
- Другие приложения, выполняют запись в каталог архивного журнала, уменьшая объем доступного для архивного журнала пространства. Не используйте пространство архивного журнала для других прикладных программ, в том числе для других серверов IBM Spectrum Protect. Убедитесь, что у каждого сервера существует отдельное положение хранения, которым владеет и управляет данный сервер.

- AIX: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами
  Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.
- AIX: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов
  Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.
- AIX: Пример: оценка размера активного и архивного журналов для операций одновременной записи
  Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.
- AIX: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера
  Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.
- AIX: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности
  Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.
- AIX: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных
  Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного

копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.

- AIX: Пример: оценка размера активных и архивных журналов для операций дедупликации данных
  Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

AIX: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами

Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.

Чтобы определить размеры активных и архивных журналов для основных операций сохранения, выполняемых клиентами, используйте следующую формулу:

```
число клиентов  x  число файлов, сохраненных в течение каждой транзакции
  x  размер пространства журнала, необходимый для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Основные операции сохранения данных клиентами

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053 байта	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	19,5 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 байт = 3,5 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`3,5 + 16 = 19,5 ГБ`

Элемент	Значения примера	Описание

Архивный журнал: Рекомендуемый размер	58,5 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала.
		`3,5 x 3 = 10,5 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`10,5 + 48 = 58,5 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

AIX: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов

Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.

Чтобы определить размеры активных и архивных журналов, когда клиенты используют несколько сеансов, примените следующую формулу:

```
число клиентов  x  число сеансов для каждого клиента  x  число файлов, сохраненных
  в течение каждой транзакции  x  объем памяти журнала, необходимой для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Несколько сеансов клиента

Элемент	Значения примера		Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	1000	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Возможных сеансов для каждого клиента	3	3	Параметр опции клиента RESOURCEUTILIZATION больше, чем значение по умолчанию. Каждый сеанс клиента запускает параллельно до трех сеансов.
Количество файлов, сохраняемых за каждую транзакцию	4096	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Элемент	Значения примера		Описание
Размер пространства журналов, необходимый для каждого файла	3053	3053	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	26,5 ГБ [1]	51 ГБ [1]	Следующие вычисления проведены для 300 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(300 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 10,5 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`10,5 + 16 = 26,5 ГБ`
			
			Следующие вычисления проведены для 1000 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(1000 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 35 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`35 + 16 = 51 ГБ`

Архивный журнал: Рекомендуемый размер	79,5 ГБ [1]	153 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
			
			`10,5 x 3 = 31,5 ГБ`
			
			`35 x 3 = 105 ГБ`
			
			Увеличим эти размеры на рекомендуемый начальный размер 48 ГБ:
			
			`31,5 + 48 = 79,5 ГБ`
			
			`105 + 48 = 153 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте ваш активный журнал и при необходимости настраивайте его размер.

AIX: Пример: оценка размера активного и архивного журналов для операций одновременной записи

Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.

Пространство журнала, требуемое для каждого файла, увеличивается примерно на 200 байт на каждый пул хранения копий, который используется для операции одновременной записи. В примере в следующей таблице данные сохраняются в двух пулах хранения копий в дополнение к первичному пулу хранения. Оценочный размер журнала увеличивается на 400 байт для каждого файла. Если использовать рекомендованное значение памяти журнала для каждого файла (3053 байта), полный объем составит 3453 байта.

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Одновременные операции записи

Элемент	**Значения примера**	**Описание**
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байта на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3453 байта на каждый файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Элемент	Значения примера	Описание

Архивный журнал: Рекомендуемый размер	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить требования к размеру архивного журнала:
		`4 ГБ x 3 = 12 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`12 + 48 = 60 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

AIX: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера

Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.

Например, перемещение данных из дискового пула хранения с произвольным доступом (DISK) в дисковый пул хранения с последовательным доступом (FILE) использует примерно 110 байт памяти журнала на каждый перемещаемый файл. Допустим, например, что у вас есть 300 клиентов архивирования и резервного копирования, и каждый из них проводит резервное копирование 100 000 файлов каждую ночь. Файлы изначально хранятся в пуле хранения DISK, а затем переносятся в пул хранения FILE. Чтобы оценить объем памяти активного журнала, требуемой для этого перемещения данных, воспользуемся следующим вычислением. Число клиентов в формуле представляет собой максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время.

```
300 клиентов  x 100 000 файлов на каждого клиента  x  110 байт =  3,1 ГБ
```

Добавьте это значение к оценке размера активного журнала, полученной для основных операций сохранения данных клиентами.

AIX: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности

Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.

AIX: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных

Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.

Например, если полное резервное копирование базы данных производится раз в неделю, размер архивного журнала должен быть достаточным, чтобы содержать всю информацию за неделю в архивном журнале.

Различие в размерах архивного журнала для ежедневных и полных резервных копирований базы данных показано в примере в следующей таблице.

Табл. 1. Полное резервное копирование базы данных

Элемент	**Значения примера**	**Описание**
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байт на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 файлов на транзакцию x 3453 байт на файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Элемент	Значения примера	Описание

Архивный журнал: Рекомендованный размер при ежедневном полном резервном копировании базы данных	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
		`4 ГБ x 3 = 12 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`12 + 48 = 60 ГБ`

Архивный журнал: Рекомендованный размер при еженедельном полном резервном копировании базы данных	132 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала. Умножим этот результат на число дней между полными резервными копированиями базы данных:
		`(4 ГБ x 3 ) x 7 = 84 ГБ`
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		`84 + 48 = 132 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Рекомендуемый начальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

AIX: Пример: оценка размера активных и архивных журналов для операций дедупликации данных

Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Следующие факторы влияют на требования к размеру пространства активных и архивных журналов:

Объем дедуплицированных данных
: Влияние дедупликации данных на размер активного и архивного журналов зависит от процентной доли данных, которые могут использоваться для дедупликации. Если эта процентная доля данных для дедупликации относительно велика, потребуется больший объем пространства журналов.

Размер и количество экстентов
: Для каждого экстента, идентифицированного в процессе подготовки дедупликации, требуется примерно 1500 байт в пространстве активного журнала. Например, если при подготовке процесса дедупликации идентифицировано 250 тысяч экстентов, оценочный объем активного журнала составляет:

```
250 000 идентифицированных в каждом процессе экстентов x 1500 байт
 для каждого экстента = 358 МБ
```

Рассмотрим следующий сценарий: Триста клиентов архива резервных копий проводят каждую ночь до 100 тысяч операций резервного копирования файлов. Эти операции создают рабочую нагрузку в 30 миллионов файлов. Среднее количество экстентов для каждого файла - два. Следовательно, полное число экстентов - 60 миллионов, а для архивного журнала требуется 84 ГБ памяти:

```
60 000 000 экстентов x 1500 байт на каждый экстент = 84 ГБ
```

Процесс идентификации дубликатов оперирует с агрегатами файлов. Агрегат состоит из файлов, которые сохранены в данной транзакции, как задано опцией сервера TXNGROUPMAX. Предположим, что по умолчанию для опции сервера TXNGROUPMAX задано значение 4096. Если среднее число экстентов для каждого файла - два, общее число экстентов в каждом агрегате - 8192, а требуемая память активного журнала - 12 МБ:

```
8192 экстента в каждом агрегате x 1500 байт на каждый экстент =
   12 МБ
```

Время выполнения и число процессов идентификации дубликатов

Время выполнения и число процессов идентификации дубликатов также влияют на размер активного журнала. Если использовать оцененный в предыдущем примере размер активного журнала (12 МБ), при параллельном выполнении десяти процессов идентификации дубликатов одновременная нагрузка активного журнала составит 120 МБ:

```
12 МБ на каждый процесс x 10 процессов = 120 МБ
```

Размер файла

На размер активного журнала могут влиять также большие файлы, обрабатываемые для идентификации дубликатов. Допустим, например, что клиент резервного копирования и архивирования производит резервную копию около 80 гигабайтов (снимок файловой системы). В этом объекте может содержаться большое число дублированных экстентов, например, если проводилось инкрементное резервное копирование включенных в файловую систему файлов. Допустим, например, что снимок файловой системы содержит 1,2 миллиона дублированных экстентов. Эти 1,2 миллиона экстентов в таком большом файле представляют единственную транзакцию для процесса идентификации дубликатов. Требуемая для этого единственного объекта полная память активного журнала составляет 1,7 гигабайтов:

```
1 200 000 экстентов x 1500 байт на каждый экстент = 1,7 ГБ
```

Если одновременно с процессом идентификации дубликатов для этого большого объекта будет происходит аналогичный, но меньший по объему процесс, активному журналу может не хватить памяти. Допустим, например, что пул хранения включен для дедупликации. В пуле хранения содержится смесь данных, в том числе мелкие файлы с размером от 10 КБ до нескольких сотен КБ. В пуле хранения есть также несколько больших объектов, содержащих основную процентную долю дублированных экстентов.

Чтобы принять во внимание не только требования к объему памяти, но и затраты времени и продолжительность одновременных транзакций, увеличьте оцененный размер активного журнала примерно вдвое. Допустим, например, что ваша оценка дает для требуемого объема памяти значение 25 ГБ (23,3 ГБ + 1,7 ГБ на дедупликацию большого объекта). Если процессы дедупликации выполняются одновременно, рекомендуемый размер активного журнала составит 50 ГБ. Предлагаемый размер архивного журнала - 150 ГБ.

Примеры в следующих таблицах показывают результаты расчетов для активных и архивных журналов. В примере первой таблицы использован средний размер экстента 700 КБ. Во втором примере (вторая таблица) средний размер экстента - 256 КБ. Как видно, меньший средний размер дубликата экстента (256 КБ) приводит к большему оцененному размеру активного журнала. Для исключения или минимизации проблем функционирования сервера используйте значение 256 КБ для оценки размера активного журнала в вашей производственной среде.

Табл. 1. Средний размер дубликата экстента - 700 КБ

Элемент	**Значения примера**		**Описание**
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	700 КБ	700 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.

Элемент	Значения примера		Описание
Экстенты для данного файла	1 198 372 бит	6 135 667 бит	При использовании среднего размера экстентов (700 КБ) эта оценка дает среднее число экстентов для данного объекта. Для объекта размером 800 ГБ была использована следующая формула: `(800 ГБ ÷ 700 КБ) = 1 198 372 бит` Аналогичные вычисления для объекта размером 4 ТБ: `(4 ТБ ÷ 700 КБ) = 6 135 667`
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	1,7 ГБ	8,6 ГБ	Оценка размера активного журнала, требуемого для этой транзакции.

Активный журнал: Рекомендуемый общий размер	66 ГБ [1]	79,8 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 1,7 ГБ) x 2 = 50 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`50 + 16 = 66 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 8,6 ГБ) x 2 = 63,8 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`63,8 + 16 = 79,8 ГБ`

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	198 ГБ [1]	239,4 ГБ [1]	Увеличьте оцененный размер активного журнала втрое.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`50 ГБ x 3 = 150 ГБ`
			
			Увеличим этот размер на рекомендуемый начальный размер 48 ГБ:
			
			`150 + 48 = 198 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`63,8 ГБ x 3 = 191,4 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`191,4 + 48 = 239,4 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Табл. 2. Средний размер дубликата экстента - 256 КБ

Элемент	Значения примера		Описание
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	256 КБ	256 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.

Экстенты для данного файла	3 276 800 бит	16 777 216 бит	При использовании среднего размера экстентов эта оценка дает среднее число экстентов для данного объекта.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(800 ГБ ÷ 256 КБ) = 3 276 800 бит`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(4 ТБ ÷ 256 КБ) = 16 777 216 бит`

Элемент	Значения примера		Описание
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	4,5 ГБ	23,4 ГБ	Оценочный размер памяти активного журнала, требуемой для этой транзакции.

Активный журнал: Рекомендуемый общий размер	71,6 ГБ [1]	109,4 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 4,5 ГБ) x 2 = 55,6 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`55,6 + 16 = 71,6 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 23,4 ГБ) x 2 = 93,4 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`93,4 + 16 = 109,4 ГБ`

Архивный журнал: Рекомендуемый размер	214,8 ГБ [1]	328,2 ГБ [1]	Троекратный размер оценки активного журнала.
			
			Следующие вычисления проведены для объекта размером 800 ГБ:
			
			`55,6 ГБ x 3 = 166,8 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`166,8 + 48 = 214,8 ГБ`
			
			Следующие вычисления проведены для объекта размером 4 ТБ:
			
			`93,4 ГБ x 3 = 280,2 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`280,2 + 48 = 328,2 ГБ`

Элемент	Значения примера	Описание
[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.		

AIX: Пространство зеркальной копии активного журнала

Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.

Создание зеркальной копии журнала - рекомендуемая опция. Если вы увеличите размер активного журнала, размер зеркальной копии журнала увеличится автоматически. Зеркальное копирование журнала может отрицательно сказаться на производительности, так как при зеркальном копировании потребуется удвоенный объем операций ввода-вывода. Дополнительное пространство, которое требуется для зеркальной копии журнала - это еще один фактор, который следует учесть, при принятии решения относительно создания зеркальной копии журнала.

Если каталог зеркальной копии журнала переполняется, сервер записывает сообщения об ошибке в активный журнал и в файл db2diag.log. Работа сервера продолжится.

AIX: Пространство резервного архивного журнала

Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Задав каталог резервного архивного журнала, можно предотвратить ошибки, которые могут происходить при нехватке места в каталоге архивного журнала. Если переполнятся и каталог архивного журнала, и диск или файловая система, где находится каталог резервного архивного журнала, данные останутся в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением активного журнала.

AIX: Мониторинг использования пространства для базы данных и журналов восстановления

Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.

Активный журнал

Если объем доступного пространства активного журнала недостаточен, в журнале операций появятся следующие записи:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Сервер IBM Spectrum Protect начинает полное резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Надо вручную выполнить резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER

Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Если должно будет начаться хотя бы одно полное резервное копирование базы данных, сервер IBM Spectrum Protect начнет инкрементное резервное копирование базы данных. В противном случае сервер начнет полное резервное копирование базы данных.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Надо вручную выполнить резервное копирование базы данных.

Архивный журнал

Если объем доступного пространства архивного журнала недостаточен, в журнале операций появится следующая запись:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Отношение размера используемого пространства архивного журнала к доступному размеру пространства архивного журнала превышает порог использования журнала. Сервер IBM Spectrum Protect начинает автоматическое полное резервное копирование базы данных.

Database

Если объем доступного пространства для операций базы данных недостаточен, в журнале операций появятся следующие сообщения:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Используемое пространство базы данных превышает порог использования пространства базы данных. Чтобы увеличить размер пространства для базы данных, используйте команду EXTEND DBSPACE, команду EXTEND DBSPACE или утилиту DSMSERV FORMAT с параметром DBDIR.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Размер доступного пространства в каталоге, где расположены серверные файлы базы данных, меньше 1 ГБ.

Когда сервер IBM Spectrum Protect создается при помощи утилиты DSMSERV FORMAT или мастера по конфигурированию, одновременно создаются база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных. Указанный в этом сообщении каталог обозначает положение информации о базе данных, используемой менеджером баз данных. Если в этом каталоге нет доступного пространства, сервер больше не может функционировать.

Необходимо добавить пространство к файловой системе или обеспечить доступное пространство в файловой системе или на диске.

AIX: Удаление файлов отката установки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Об этой задаче

Чтобы удалить файлы, которые больше не нужны, используйте либо графический мастер установки, либо командную строку в режиме консоли.

- AIX: Удаление файлов отката установки с использованием графического мастера
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.
- AIX: Удаление файлов отката установки с использованием командной строки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

AIX: Удаление файлов отката установки с использованием графического мастера

Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.

Процедура

1. Откройте IBM Installation Manager.
   Операционные системы AIXВ каталоге, в котором установлен IBM Installation Manager, перейдите в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду, чтобы запустить IBM Installation Manager:

   ```
   ./IBMIM
   ```

2. Щелкните по Файл > Предпочтения.
3. Выберите Файлы для отката.
4. Щелкните по Удалить сохраненные файлы и нажмите на OK.

AIX: Удаление файлов отката установки с использованием командной строки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Процедура

1. В каталоге, в котором установлен IBM® Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы AIXeclipse/tools

   Например:

   - Операционные системы AIX/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду, чтобы запустить командную строку IBM Installation Manager:
   - Операционные системы AIX`./imcl -c`
3. Введите `П`, чтобы выбрать Предпочтения.
4. Введите `3`, чтобы выбрать Файлы для отката.
5. Введите `D`, чтобы удалить файлы для отката.
6. Введите `A`, чтобы применить изменения и вернуться в меню предпочтений.
7. Введите `C`, чтобы выйти из Меню предпочтений.
8. Введите `X`, чтобы закрыть Installation Manager.

AIX: Практические рекомендации по именованию сервера

Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.

ID пользователя экземпляра

ID пользователя экземпляра служит основой для других имен, связанных с экземпляром сервера. ID пользователя экземпляра также называют владельцем экземпляра.

Например: tsminst1

ID пользователя экземпляра - это ID пользователя, у которого должны быть полномочия владельца или доступ с правом на чтение/запись для всех каталогов, которые вы создаете для базы данных и журнала восстановления. Обычная практика работы сервера - его запуск от имени ID пользователя экземпляра. У этого ID пользователя должно быть право чтения и записи в каталоги, используемые для всех классов устройств FILE.

Операционные системы AIX

Домашний каталог для ID пользователя экземпляра

Домашний каталог (если он еще не существует) можно создать при создании ID пользователя экземпляра, указав для этого опцию -m. В зависимости от локальных параметров имя домашнего каталога может иметь следующий

вид: /home/*ID_пользователя_экземпляра*.

Например: /home/tsminst1

Домашний каталог изначально используется для содержания профиля ID пользователя и параметров безопасности.

 Операционные системы AIX

Имя экземпляра базы данных

Имя экземпляра базы данных должно совпадать с ID пользователя экземпляра, от имени которого вы запускаете экземпляр сервера.

Например: tsminst1

 Операционные системы AIX

Каталог экземпляра

Каталог экземпляра - это каталог, содержащий связанные с экземпляром сервера файлы (файл опций сервера и другие специфичные для сервера файлы). У этого каталога может быть любое имя по вашему выбору. Чтобы этот каталог было проще распознать, используйте имя, связывающее каталог с именем экземпляра.

Каталог экземпляра можно создать как подкаталог домашнего каталога ID пользователя экземпляра. Например: /home/*ID_пользователя_экземпляра*/*ID_пользователя_экземпляра*

В приведенном ниже примере каталог экземпляра размещается в домашнем каталоге для пользователя с ID tsminst1: /home/tsminst1/tsminst1

Этот каталог также можно создать в другом месте, например: /tsmserver/tsminst1

В каталоге экземпляра хранятся следующие файлы для экземпляра сервера:

- Файл серверных опций, dsmserv.opt
- Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
- Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
- Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
- Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.
- Обработчики пользователя
- Выходная информация трассировки (если не задано полное имя)

Имя базы данных

Именем базы данных для каждого экземпляра сервера всегда является TSMDB1. Это имя нельзя изменить.

Имя сервера

Имя сервера - это внутреннее имя для IBM Spectrum Protect, и оно используется для выполнения операций, включающих в себя взаимодействия между несколькими серверами IBM Spectrum Protect. В качестве примера можно привести взаимодействие сервера с сервером и совместное использование библиотеки.

 Операционные системы AIXИмя сервера также используется при добавлении сервера в Центр операций, чтобы им можно было управлять с использованием этого интерфейса. Используйте для каждого сервера уникальное имя. Чтобы имя было проще распознать в Центре операций или в выходной информации команды QUERY SERVER, используйте имя, отражающее положение или назначение сервера. Не изменяйте имя сервера IBM Spectrum Protect после того, как он сконфигурирован как хаб или подчиненный сервер.

Если вы используете мастер, рекомендуемым именем по умолчанию будет имя хоста компьютера, который вы используете. Можно использовать другое имя, которое будет иметь смысл в вашей среде. Если у вас в системе более одного сервера и вы используете мастер, вы сможете использовать имя по умолчанию только для одного из серверов. Для каждого сервера нужно ввести уникальное имя.

Операционные системы AIXНапример:

- PAYROLL
- SALES

Каталоги для пространства базы данных и журнала восстановления

Каталогам можно присваивать имена в соответствии с принятой у вас практикой. Чтобы было проще распознавать каталоги, используйте имена, связывающие каталоги с экземпляром сервера.

Например, в случае архивного журнала:

- Операционные системы AIX/tsminst1_archlog

AIX: Каталоги установки

К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

(/opt/tivoli/tsm/server/bin) - это каталог по умолчанию, содержащий код сервера и файлы лицензии.

Структура каталогов продукта DB2, устанавливаемого в ходе установки сервера IBM Spectrum Protect, соответствует тому, что задокументировано в источниках информации по DB2. Защищайте эти каталоги и файлы так же, как вы защищаете каталоги сервера. Каталог по умолчанию - /opt/tivoli/tsm/db2.

Можно использовать следующий языки: английский (США), испанский, итальянский, китайский Big5, китайский GBK, китайский традиционный, китайский упрощенный, корейский, немецкий, португальский (Бразилия), русский, французский и японский.

AIX: Установка компонентов сервера

Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.

Об этой задаче

При использовании программы установки IBM Spectrum Protect можно установить следующие компоненты:

- сервер (server)
  Совет: База данных (DB2), Global Security Kit (GSKit) и IBM® Java™ Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- языки сервера
- лицензия
- устройства
- IBM Spectrum Protect for SAN
- Центр операций

Операционные системы AIXДля установки сервера версии 8.1.5 надо выделить примерно 30 - 45 минут.

- AIX: Получение пакета установки
  Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM (например, Passport Advantage или IBM Fix Central).
- AIX: Установка IBM Spectrum Protect при помощи мастера установки
  Сервер можно установить при помощи графического мастера IBM Installation Manager.
- AIX: Установка IBM Spectrum Protect в режиме консоли
  IBM Spectrum Protect можно установить из командной строки в режиме консоли.
- AIX: Установка IBM Spectrum Protect в режиме без вывода сообщений
  Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.
- AIX: Установка языковых пакетов сервера
  Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского

(США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

AIX: Получение пакета установки

Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM® (например, Passport Advantage или IBM Fix Central).

 Операционные системы AIX

Прежде чем начать

Если вы собираетесь скачать эти файлы, задайте неограниченный системный предел пользователя для максимального размера файла, чтобы файлы были успешно скачаны:

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

   ```
   ulimit -Hf
   ```

2. Если системный пользовательский предел на максимальный размер файла не задан неограниченным, измените его на неограниченный, следуя инструкциям в документации для вашей операционной системы.

Процедура

1. Загрузите нужный файл пакета с одного из следующих веб-сайтов.
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.
   - Самую свежую информацию, обновления и исправления обслуживания смотрите по адресу: Портал поддержки IBM.
2. Если вы скачали пакет с сайта скачивания IBM, то сделайте следующее:
   Операционные системы AIX
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к свободному месту можно увидеть в документе по скачиванию:
      - IBM Spectrum Protect техническое замечание 4042944
      - IBM Spectrum Protect Extended Edition техническое замечание 4042945
      - IBM Spectrum Protect for Data Retention техническое замечание 4042946

   b. Скачайте файл пакета в каталог по вашему выбору. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.
   c. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

      ```
      chmod a+x имя_пакета.bin
      ```

   d. Извлеките пакет, введя следующую команду:

      ```
      ./имя_пакета.bin
      ```

      где *имя_пакета* - это имя скачанного файла, например:

       Операционные системы AIX

      ```
      8.1.x.000-IBM-SPSRV-AIX.bin
      ```

3.  Операционные системы AIXУбедитесь, что включена следующая команда, так что мастера IBM Spectrum Protect работают правильно:
   -  Операционные системы AIX`lsuser`

   По умолчанию эта команда включена.
4. Выберите один из следующих способов установки IBM Spectrum Protect:
   - AIX: Установка IBM Spectrum Protect при помощи мастера установки
   - AIX: Установка IBM Spectrum Protect в режиме консоли
   - AIX: Установка IBM Spectrum Protect в режиме без вывода сообщений
5. После установки IBM Spectrum Protect и до настройки этого продукта в соответствии с вашими требованиями посетите следующий веб-сайт: Портал поддержки IBM. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

AIX: Установка IBM Spectrum Protect при помощи мастера установки

Сервер можно установить при помощи графического мастера IBM® Installation Manager.

Прежде чем начать

Перед запуском установки сделайте следующее:

-  Если перечисленные ниже файлы RPM не установлены на компьютере, то установите их. Инструкции смотрите в разделе Установка файлов RPM для графического мастера.
  - atk-1.12.3-2.aix5.2.ppc.rpm
  - cairo-1.8.8-1.aix5.2.ppc.rpm
  - expat-2.0.1-1.aix5.2.ppc.rpm
  - fontconfig-2.4.2-1.aix5.2.ppc.rpm
  - freetype2-2.3.9-1.aix5.2.ppc.rpm
  - gettext-0.10.40-6.aix5.1.ppc.rpm
  - glib2-2.12.4-2.aix5.2.ppc.rpm
  - gtk2-2.10.6-4.aix5.2.ppc.rpm
  - libjpeg-6b-6.aix5.1.ppc.rpm
  - libpng-1.2.32-2.aix5.2.ppc.rpm
  - libtiff-3.8.2-1.aix5.2.ppc.rpm
  - pango-1.14.5-4.aix5.2.ppc.rpm
  - pixman-0.12.0-3.aix5.2.ppc.rpm
  - xcursor-1.1.7-3.aix5.2.ppc.rpm
  - xft-2.1.6-5.aix5.1.ppc.rpm
  - xrender-0.9.1-3.aix5.2.ppc.rpm
  - zlib-1.2.3-3.aix5.1.ppc.rpm
- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки, введя следующую команду:  Операционные системы AIX `./install.sh`

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Вы можете просмотреть файлы журнала установки, выбрав Файл > Просмотреть журнал в инструменте Installation Manager. Чтобы выполнить сбор этих файлов журнала, выберите Справка > Экспорт данных для анализа проблем в инструменте Installation Manager.

- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.

-  Операционные системы AIXПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

-  Операционные системы AIXAIX: Установка обязательных файлов RPM для графического мастера
  Чтобы можно было использовать графический мастер IBM Installation Manager для установки IBM Spectrum Protect, нужно установить обязательные файлы RPM.

AIX: Установка IBM Spectrum Protect в режиме консоли

IBM Spectrum Protect можно установить из командной строки в режиме консоли.

Прежде чем начать

Перед запуском установки сделайте следующее:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки в консольном режиме, введя следующую команду: Операционные системы AIX `./install.sh -c` Необязательно: Сгенерируйте файл ответов в ходе установки в режиме консоли. Укажите опции установки в режиме консоли и на панели Сводка укажите `G`, чтобы сгенерировать ответы.

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  - Операционные системы AIX/var/ibm/InstallationManager/logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
- Операционные системы AIXПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

AIX: Установка IBM Spectrum Protect в режиме без вывода сообщений

Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге input в том месте, куда был распакован пакет установки:

install_response_sample.xml
: Используйте этот файл для установки компонентов IBM Spectrum Protect.

update_response_sample.xml
: Используйте этот файл для обновления компонентов IBM Spectrum Protect.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов. Вы можете изменить пример файла ответов или создать свой собственный.
2. Если вы устанавливаете сервер и компонент Центр операций в режиме без вывода сообщений, создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.
   Если вы используете файл install_response_sample.xml, добавьте пароль в следующую строку в файле, где *пароль* - это пароль:

   ```
   <variable name='ssl.password' value='пароль' />
   ```

   Дополнительную информацию об этом пароле смотрите в разделе Контрольный список установки.
   Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл update_response_sample.xml для обновления компонента Центр операций.
3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:
   -  Операционные системы AIX

     ```
     ./install.sh -s -input файл_ответов
     -acceptLicense
     ```

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  -  Операционные системы AIX/var/ibm/InstallationManager/logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
-  Операционные системы AIXПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

 Операционные системы AIX

AIX: Установка языковых пакетов сервера

Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Прежде чем начать

Инструкции по установке пакетов поддержки национальных языков для агента хранения смотрите в документе Конфигурация пакета поддержки национальных языков для агентов хранения.

- AIX: Локали языка сервера
  Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.
- AIX: Конфигурирование языкового пакета
  После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.
- AIX: Обновление языкового пакета
  Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

AIX: Локали языка сервера

Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.

 Операционные системы AIXЭтот языковый пакет автоматически устанавливается для следующей языковой опции по умолчанию для сообщений и справки сервера IBM Spectrum Protect:

-  Операционные системы AIXLANGUAGE en_US

Для прочих языков и локалей установите языковой пакет, нужный для вашей установки.
Можно использовать следующие языки:
Операционные системы AIX

Табл. 1. Языки сервера для AIX

Язык	Значение опции LANGUAGE
Китайский упрощенный	zh_CN
Китайский упрощенный (UTF-8)	ZH_CN
Китайский традиционный (Big5)	Zh_TW
Китайский традиционный (UTF-8)	ZH_TW
Китайский традиционный (euc_tw)	zh_TW
Английский	en_US
Английский (UTF-8)	EN_US
Французский	fr_FR
Французский (UTF-8)	FR_FR
Немецкий	de_DE
Немецкий (UTF-8)	DE_DE
Итальянский	it_IT
Итальянский (UTF-8)	IT_IT
Японский, EUC	ja_JP
Японский, PC	Ja_JP
Японский, UTF8	JA_JP
Корейский	ko_KR
Корейский (UTF-8)	KO_KR
Бразильский португальский	pt_BR
Бразильский португальский (UTF-8)	PT_BR
Русский	ru_RU
Русский (UTF-8)	RU_RU
Испанский	es_ES
Испанский (UTF-8)	ES_ES

Операционные системы AIXОграничение: При использовании Центр операций некоторые символы могут выводиться неправильно, если язык веб-браузера не совпадает с языком сервера. При появлении этой неполадки следует сконфигурировать в браузере использование того же языка, что и на сервере.

AIX: Конфигурирование языкового пакета

После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.

Об этой задаче

Операционные системы AIXДля задания поддержки определенной локали выполните одну из следующих задач:

- Для опции LANGUAGE в файле опций сервера задайте имя локали, которую нужно использовать. Например:
  - Операционные системы AIXЧтобы использовать локаль `ru_RU.UTF-8`, задайте для опции LANGUAGE значение `ru_RU.UTF-8`. Смотрите раздел AIX: Локали языка сервера.
- Операционные системы AIXЕсли вы запускаете сервер в режиме активного окна, то задайте для переменной среды `LC_ALL` значение, совпадающее со значением, которое задано в файле опций сервера. Например, чтобы задать переменную среды для русского языка, введите следующее значение:

```
export LC_ALL=ru_RU.UTF-8
```

Если локаль успешно инициализирована, то с ее помощью форматируется дата, время и представление чисел для сервера. Если локаль не инициализируется успешно, сервер будет использовать файлы сообщений на английском языке (США), а также формат дат времени и чисел для языка системы 'Английский (США)'.

AIX: Обновление языкового пакета

Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

Об этой задаче

Внутри одного и того же экземпляра IBM Spectrum Protect можно установить другой языковой пакет.

- Для установки другого языкового пакета используйте функцию Изменить программы IBM Installation Manager.
- Для обновления языковых пакетов до новых версий используйте функцию Обновить программы IBM Installation Manager.

Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* являются синонимами.

AIX: Первые шаги после установки IBM Spectrum Protect

После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.

Об этой задаче

1. Создайте каталоги и ID пользователя для экземпляра сервера. Смотрите раздел AIX: Создание ID пользователя и каталогов для экземпляра сервера.
2. Сконфигурируйте экземпляр сервера. Выберите одну из следующих опций.
    - Воспользуйтесь мастером по конфигурированию - это рекомендуемый способ. Смотрите раздел AIX: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования.
    - Сконфигурируйте вручную новый экземпляр. Смотрите раздел AIX: Конфигурирование экземпляра сервера вручную. При конфигурировании вручную выполните описанные ниже шаги.
        a. Сконфигурируйте каталоги и создайте экземпляр IBM Spectrum Protect. Смотрите раздел AIX: Создание экземпляра сервера.
        b. Создайте новый файл серверных опций, скопировав пример файла, чтобы сконфигурировать связь между сервером и клиентами. Смотрите раздел Операционные системы AIXAIX: Конфигурирование связи между сервером и клиентом.
        c. Введите команду DSMSERV FORMAT, чтобы сформатировать базу данных. Смотрите раздел AIX: Форматирование базы данных и журнала.
        d. Сконфигурируйте систему для резервного копирования базы данных. Смотрите раздел AIX: Подготовка менеджера базы данных к резервному копированию базы данных.
3. Сконфигурируйте опции, чтобы задать, когда запускать реорганизацию базы данных. Смотрите раздел AIX: Опции конфигурирования сервера для обслуживания сервера баз данных.
4. Запустите экземпляр сервера, если он еще не запущен.
    - Операционные системы AIXСмотрите раздел AIX: Запуск экземпляра сервера.
5. Зарегистрируйте свою лицензию. Смотрите раздел AIX: Регистрация лицензий.
6. Подготовьте систему для резервного копирования базы данных. Смотрите раздел AIX: Подготовка сервера к операциям резервного копирования базы данных.
7. Наблюдайте сервер. Смотрите раздел AIX: Мониторинг сервера.

- AIX: Создание ID пользователя и каталогов для экземпляра сервера
  Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.
- AIX: Конфигурирование сервера IBM Spectrum Protect
  После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.
- AIX: Опции конфигурирования сервера для обслуживания сервера баз данных
  Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный

режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

-  Операционные системы AIXAIX: Запуск экземпляра сервера
  Сервер можно запускать от имени ID пользователя экземпляра (что является предпочтительным методом) или от имени ID пользователя root.
- AIX: Остановка сервера
  При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.
- AIX: Регистрация лицензий
  Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.
- AIX: Подготовка сервера к операциям резервного копирования базы данных
  Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.
- AIX: Запуск нескольких экземпляров серверов на одном компьютере
  Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.
- AIX: Мониторинг сервера
  Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

AIX: Создание ID пользователя и каталогов для экземпляра сервера

Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.

Прежде чем начать

Прежде чем выполнять данную задачу, ознакомьтесь с информацией о планировании пространства для сервера. Смотрите раздел AIX: Контрольные списки для планирования сведений о сервере.

Процедура

1. Создайте ID пользователя, который станет владельцем экземпляра сервера. Вы будете использовать этот ID пользователя при создании экземпляра сервера в одном из последующих шагов.

    Операционные системы AIX
    Операционные системы AIXСоздайте ID пользователя и группу, которые станут владельцем экземпляра сервера.
   a. От имени ID пользователя - администратора можно запустить следующие команды конфигурирования пользователей и групп. Создайте ID пользователя и группу в домашнем каталоге пользователя. Ограничение: В ID пользователя можно использовать буквы нижнего регистра (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:
      - Длина не должна превышать 8 символов.
      - ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
      - В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

      Например, создайте ID пользователя `tsminst1` в группе `tsmsrvrs`. В приведенных ниже примерах показано, как создать этот ID пользователя и эту группу при помощи команд операционной системы.

       Операционные системы AIX

      ```
      mkgroup id=1001 tsmsrvrs
      mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
      passwd tsminst1
      ```

      Ограничение: DB2 не поддерживает непосредственную аутентификацию пользователя системы через LDAP.

b. Выйдите из системы, затем снова в нее войдите. Перейдите на только что созданную учетную запись пользователя. Используйте интерактивную программу входа в систему, например, telnet, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.

2. Создайте каталоги, необходимые серверу.
 Операционные системы AIXСоздайте пустые каталоги для каждого элемента в таблице и убедитесь, что каталогами владеет новый ID пользователя, который вы только что создали. Смонтируйте связанную систему хранения каждому каталогу для активного и архивного журнала, а также для каталогов базы данных.

Элемент	**Примеры команд для создания каталогов**	**Ваши каталоги**
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)	`mkdir /tsminst1`	

Каталоги базы данных	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Каталог активного журнала	`mkdir /tsmlog`	
Каталог архивного журнала	`mkdir /tsmarchlog`	
Необязательно: Каталог для зеркальной копии активного журнала	`mkdir /tsmlogmirror`	
Необязательно: Каталог вторичного архивного журнала (каталог для резервного архивного журнала)	`mkdir /tsmarchlogfailover`	

При первоначальном создании сервера при помощи утилиты DSMSERV FORMAT или мастера конфигурирования создается база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных.

3. Завершите сеанс для нового ID пользователя.

AIX: Конфигурирование сервера IBM Spectrum Protect

После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.

Об этой задаче

Сконфигурируйте экземпляр сервера IBM Spectrum Protect, выбрав один из следующих вариантов:

- AIX: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования
  Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.
- AIX: Конфигурирование экземпляра сервера вручную
  После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

AIX: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования

Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите

мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.

Прежде чем начать

Прежде чем использовать мастер конфигурирования, нужно выполнить все предыдущие шаги для подготовки к конфигурированию. В число этих шагов входят установка IBM Spectrum Protect, создание каталогов базы данных и журналов и создание каталогов и ID пользователя для экземпляра сервера.

Процедура

1. Убедитесь, что выполнены следующие требования:
    Операционные системы AIX
   - В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
   - В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле `sshd_config` в каталоге /etc/ssh/. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения `localhost`.
   - Вы должны иметь возможность войти в систему, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
   - Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
     - Файлы главного ключа шифрования (`dsmkeydb.*`)
     - Сертификат сервера и файлы секретных ключей (`cert.*`)
2. Запустите локальную версию мастера:
   -  Операционные системы AIXОткройте программу `dsmicfgx` в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запускать только с использованием ID пользователя root.

   Завершите конфигурирование, следуя инструкциям. Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

AIX: Конфигурирование экземпляра сервера вручную

После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

- AIX: Создание экземпляра сервера
  Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.
-  Операционные системы AIXAIX: Конфигурирование связи между сервером и клиентом
  Пример файла серверных опций по умолчанию, dsmserv.opt.smp, создается в каталоге /opt/tivoli/tsm/server/bin при установке IBM Spectrum Protect. Вы должны сконфигурировать связь между сервером и клиентами, создав новый файл серверных опций. Для этого скопируйте пример файла в каталог экземпляра сервера.
- AIX: Форматирование базы данных и журнала
  Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.
- AIX: Подготовка менеджера базы данных к резервному копированию базы данных
  Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

AIX: Создание экземпляра сервера

Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.

Об этой задаче

На одной рабочей станции может быть один или несколько экземпляров сервера.
Операционные системы AIXВажное замечание: Прежде чем вводить команду db2icrt, убедитесь в следующем:

- Существует домашний каталог для пользователя (/home/tsminst1). Если домашнего каталога нет, вы должны его создать.
  В каталоге экземпляра хранятся следующие файлы, сгенерированные сервером IBM Spectrum Protect:
  - Файл серверных опций, dsmserv.opt
  - Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
  - Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
  - Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
  - Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.
  - Обработчики пользователя
  - Выходная информация трассировки (если не задано полное имя)
- Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
  - Файлы главного ключа шифрования (`dsmkeydb.*`)
  - Сертификат сервера и файлы секретных ключей (`cert.*`)
- У пользователя root и ID пользователя экземпляра должны быть разрешения на запись в файл конфигурации оболочки. В домашнем каталоге существует файл конфигурации оболочки (например, .profile). Дополнительную информацию смотрите на веб-сайте Информация о DB2. Найдите информацию о переменных среды Linux и UNIX.

Операционные системы AIX

1. Войдите в систему с ID пользователя root и создайте экземпляр IBM Spectrum Protect. Имя экземпляра должно совпадать с именем пользователя, являющегося владельцем экземпляра. Введите команду db2icrt в виде одной строки:Операционные системы AIX

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   имя_экземпляра имя_экземпляра
   ```

   Например, если ID пользователя данного экземпляра - tsminst1, создайте экземпляр, введя следующую команду: Введите команду в одной строке.Операционные системы AIX

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Напоминание: С этого момента используйте этот новый ID пользователя при конфигурировании сервера IBM Spectrum Protect. Завершите сеанс ID пользователя root и войдите в систему от имени нового ID пользователя-владельца экземпляра.
2. Измените каталог по умолчанию для базы данных, так чтобы он совпадал с каталогом экземпляра сервера. Если у вас несколько серверов, войдите в систему от имени ID пользователя экземпляра для каждого сервера. Введите команду:

   ```
   db2 update dbm cfg using dftdbpath каталог_экземпляра
   ```

   Например, если значением каталог_экземпляра является ID пользователя экземпляра:

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```

3. Измените путь библиотеки, включив в него библиотеки, необходимые для операций сервера.
   Совет: В следующих примерах используются следующие каталоги:
   - *каталог_bin_сервера* - это подкаталог каталога установки сервера. Например, /opt/tivoli/tsm/server/bin.
   - *домашний_каталог_пользователей_экземпляра* - это домашний каталог пользователя экземпляра. Например, /home/tsminst1.

   .
   - Операционные системы AIXВведите следующую команду в одной строке:

     ```
     export LIBPATH=каталог_bin_сервера/dbbkapi:
     /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
     ```

   - Надо изменить один из следующих файлов, чтобы задать путь библиотек, когда запускаются DB2 или сервер. Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

     Оболочка Bash или Korn:

     ```
     домашний_каталог_пользователей_экземпляра/sqllib/userprofile
     ```

     Оболочка C:

домашний_каталог_пользователей_экземпляра/sqllib/usercshrc

- Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

  Оболочка Bash или Korn:

  Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/userprofile следующую запись (в одной строке):  Операционные системы AIX

  ```
  export LIBPATH=каталог_bin_сервера/
  dbbkapi:/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  ```

  Оболочка C:

  Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/usercshrc следующую запись (на одной строке):  Операционные системы AIX

  ```
  setenv LIBPATH каталог_bin_сервера/dbbkapi:
  /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  ```

  Напоминание: В пути библиотек должны быть следующие записи, и они должны идти перед всеми другими записями в пути библиотек:
  - каталог_bin_сервера/dbbkapi
  - /usr/local/ibm/gsk8_64/lib64

4. Создайте новый файл серверных опций. Смотрите раздел AIX: Конфигурирование связи между сервером и клиентом.

 Операционные системы AIX

AIX: Конфигурирование связи между сервером и клиентом

Пример файла серверных опций по умолчанию, dsmserv.opt.smp, создается в каталоге /opt/tivoli/tsm/server/bin при установке IBM Spectrum Protect. Вы должны сконфигурировать связь между сервером и клиентами, создав новый файл серверных опций. Для этого скопируйте пример файла в каталог экземпляра сервера.

Об этой задаче

Убедитесь, что у вас есть каталог экземпляра сервера, например, /tsminst1, и скопируйте в него файл примера. Присвойте новому файлу имя `dsmserv.opt` и измените опции. Выполните это действие до инициализации базы данных сервера. Каждый образец записи или запись по умолчанию в стандартном файле опций является примечанием - строкой, начинающейся со звездочки (*). Регистр символов в именах опций не имеет значения, а между ключевыми словами и значениями можно вставлять один или несколько пробелов.

При изменении файла опций соблюдайте следующие рекомендации.

- Для активации опции удалите звездочку в начале строки.
- Для ввода опций можно использовать любой столбец.
- Одна строка должна содержать только одну опцию, а одна опция должна занимать только одну строку.
- Если одному ключевому слову соответствует несколько записей, сервер IBM Spectrum Protect использует последнюю запись.

При внесении изменений в файл опций сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Можно задать один из следующих методов связи:

- TCP/IP версии 4 или версии 6
- Совместное использование памяти
- Secure Sockets Layer (SSL)
  Совет: Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера IBM Spectrum Protect. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

-  Операционные системы AIXAIX: Задание опций TCP/IP
  Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.

- Операционные системы AIXAIX: Задание опций Shared Memory
  Вы можете использовать связь через совместную память (Shared Memory) для взаимодействия между клиентами и серверами на одном и том же компьютере. Чтобы использовать способ связи Shared Memory, в системе должен быть установлен протокол TCP/IP версии 4.
- Операционные системы AIXAIX: Задание опций Secure Sockets Layer
  Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

AIX: Задание опций TCP/IP

Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.

Об этой задаче

Ниже приводится пример списка опций TCP/IP, которые вы можете использовать для конфигурирования системы.

```
commmethod         tcpip
  tcpport            1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Совет: Можно использовать протокол TCP/IP версии 4, версии 6 или обеих версий.

TCPPORT
: Адрес порта сервера для взаимодействий TCP/IP и SSL. Значение по умолчанию - 1500.

Операционные системы AIXTCPWINDOWSIZE
: Операционные системы AIXЗадает размер буфера TCP/IP, используемого при отправке или приеме данных. Размер окна, используемого в сеансе, меньше размера окна для сервера и клиента. При большем размере окна используется дополнительная память, но это может способствовать повышению производительности.

  Можно задать целое число от 0 до 2048. Чтобы использовать размер окна по умолчанию для операционной системы, задайте значение 0.

TCPNODELAY
: Позволяет указать, будет ли сервер отправлять сообщения малого объема, или же он разрешит TCP/IP буферизовать сообщения. При отправке небольших сообщений может повыситься пропускная способность, но при этом увеличится число пакетов, отправляемых по сети. Укажите YES, чтобы отправлять короткие сообщения, или NO, чтобы протокол TCP/IP сохранял их в буфере. Значение по умолчанию - YES.

TCPADMINPORT
: Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований связи с поддержкой TCP/IP или SSL, отличных от сеансов клиентов. Значением по умолчанию является значение TCPPORT.

SSLTCPPORT
: (Только SSL) Задает номер порта Secure Sockets Layer (SSL), на котором драйвер связи TCP/IP ожидает запросы на установление сеансов SSL от клиента резервного копирования и архивирования и клиента администрирования с интерфейсом командной строки.

SSLTCPADMINPORT
: (Только SSL) Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает запросов на установление сеансов SSL от клиента администрирования с интерфейсом командной строки.

AIX: Задание опций Shared Memory

Вы можете использовать связь через совместную память (Shared Memory) для взаимодействия между клиентами и серверами на одном и том же компьютере. Чтобы использовать способ связи Shared Memory, в системе должен быть установлен протокол TCP/IP версии 4.

Об этой задаче

В приведенном ниже примере показан параметр для совместно используемой памяти (shared memory):

```
commmethod      sharedmem
   shmport      1510
```

В этом примере SHMPORT задает адрес порта TCP/IP для сервера при связи через совместно используемую память. Опцию SHMPORT можно использовать, чтобы задать другой порт TCP/IP. По умолчанию используется порт 1510.

COMMMETHOD можно использовать несколько раз в файле опций сервера IBM Spectrum Protect с различными значениями. Например, можно задать значения так:

```
commmethod         tcpip
commmethod     sharedmem
```

 Операционные системы AIXМаксимальное количество одновременных сеансов Shared Memory зависит от доступных системных ресурсов. В зависимости от уровня клиента IBM Spectrum Protect каждый сеанс Shared Memory использует одну область Shared Memory размером до 4 МБ и четыре очереди сообщений IPCS.

 Операционные системы AIXЕсли при запуске сервера и клиента использовались разные ID пользователя, то сервер должен иметь полномочия root. Это позволит избежать ошибок связи через совместную память.

AIX: Задание опций Secure Sockets Layer

Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Прежде чем начать

SSL — это стандартная технология создания зашифрованных сеансов между серверами и клиентами. SSL предоставляет безопасный канал для связи серверов и клиентов по открытым путям связи. При использовании SSL идентификационная информация сервера проверяется с помощью цифровых сертификатов.

Чтобы обеспечить оптимальную производительность системы, используйте SSL только для сеансов, где это необходимо. Добавьте на сервер IBM Spectrum Protect дополнительные ресурсы процессора, чтобы удовлетворить возросшие требования.

AIX: Форматирование базы данных и журнала

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.

После конфигурирования связей сервера все готово для инициализации базы данных. Проверьте, что вы вошли в систему под ID пользователя экземпляра. Каталоги не должны находиться в файловых системах, где может закончиться свободное пространство. Если какие-либо каталоги (например, каталог архивного журнала) окажется недоступен или переполнен, сервер остановится.

Как настроить обработчик списков завершения работы

Задайте для переменной реестра DB2NOEXITLIST значение ON для каждого экземпляра сервера. Войдите в систему от имени владельца экземпляра сервера и введите команду:

```
db2set -i имя_экземпляра_сервера
DB2NOEXITLIST=ON
```

Например:  Операционные системы AIX

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Инициализация экземпляра сервера

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. Например, если каталог экземпляра сервера - это */tsminst1*, введите следующие команды:Операционные системы AIX

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Совет: Если вы зададите несколько каталогов, убедитесь, что размеры соответствующих файловых систем равны, что позволит обеспечить непротиворечивую степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.

 Операционные системы AIXСовет: Если DB2 не запустится после ввода команды DSMSERV FORMAT, возможно, надо выключить опцию монтирования файловой системы NOSUID. Если эта опция задана для файловой системы, содержащей каталог владельца экземпляра DB2, или для файловой системы, где находится база данных DB2, активные, архивные и резервные журналы или зеркальные копии журналов, ее (опцию) нужно выключить, чтобы можно было запустить систему.
После отключения опции NOSUID повторите монтирование файловой системы и запустите DB2, введя следующую команду:

```
db2start
```

Информация, связанная с данной:
DSMSERV FORMAT (форматирование базы данных и журнала)

AIX: Подготовка менеджера базы данных к резервному копированию базы данных

Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Об этой задаче

 Операционные системы AIXНачиная с IBM Spectrum Protect V7.1.1 больше нет необходимости задавать пароль API во время конфигурирования сервера вручную. Если задать пароль API в процессе конфигурирования вручную, то попытки резервного копирования базы данных могут завершиться неудачно.

Если вы создаете экземпляр сервера IBM Spectrum Protect при помощи мастера по конфигурированию, то вам не нужно выполнять эти действия. Если вы конфигурируете экземпляр вручную, выполните описанные ниже шаги, прежде чем вводить команду BACKUP DB или RESTORE DB.

Внимание: Если база данных недоступна, весь сервер IBM Spectrum Protect становится недоступным. Если база данных утеряна и ее нельзя восстановить, может оказаться затруднительным или даже невозможным восстановить данные, которыми управляет этот сервер. Поэтому очень важно создать резервную копию базы данных.
 Операционные системы AIXВ следующих командах замените значения из примера фактическими значениями. В примерах используется значение `tsminst1` в качестве ID пользователя экземпляра сервера, /tsminst1 в качестве каталога экземпляра сервера и /home/tsminst1 в качестве домашнего каталога пользователя экземпляра сервера.

1. Задайте конфигурацию переменных среды API IBM Spectrum Protect для экземпляра базы данных:
   a. Войдите в систему от имени ID пользователя `tsminst1`.
   b. После входа пользователя `tsminst1` в систему убедитесь, что среда DB2 правильно инициализирована. Среда DB2 инициализируется путем запуска сценария /home/tsminst1/sqllib/db2profile, который обычно запускается автоматически из профиля ID пользователя. Убедитесь, что в домашнем каталоге пользователя экземпляра существует файл `.profile`, например, /home/tsminst1/.profile. Если `.profile` не запускает сценария `db2profile` добавьте в него следующие строки:

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; then
            . /home/tsminst1/sqllib/db2profile
        fi
      ```

   c. Добавьте в файл каталог_экземпляра/sqllib/userprofile следующие строки:

      ```
      DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
      DSMI_DIR=каталог_bin_сервера/dbbkapi
      DSMI_LOG=каталог_экземпляра_сервера
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      Здесь используются следующие обозначения:
      - *каталог_экземпляра* - это домашний каталог пользователя экземпляра сервера.
      - *каталог_экземпляра_сервера* - это каталог экземпляра сервера.
      - *каталог_сервера_bin* - это каталог bin сервера. Каталог по умолчанию - /opt/tivoli/tsm/server/bin.

      Добавьте в файл каталог_экземпляра/sqllib/usercshrc следующие строки:

      ```
      setenv DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
      setenv DSMI_DIR=каталог_bin_сервера/dbbkapi
      ```

```
setenv DSMI_LOG=каталог_экземпляра_сервера
```

2. Выйдите из системы и снова войдите в нее от имени `tsminst1` либо введите команду:

   ```
   . ~/.profile
   ```

   Совет: Убедитесь, что после начальной точки (.) введен пробел.
3. Создайте файл с именем `tsmdbmgr.opt` в каталоге *экземпляр_сервера*, который в этом примере находится в каталоге /tsminst1, и добавьте в него следующую строку:

   ```
   SERVERNAME TSMDBMGR_TSMINST1
   ```

   Напоминание: Значение `SERVERNAME` должно совпадать в файлах `tsmdbmgr.opt` и `dsm.sys`.
4. От имени пользователя root добавьте в файл конфигурации API IBM Spectrum Protect `dsm.sys` указанные ниже строки. По умолчанию файл конфигурации `dsm.sys` находится в следующем каталоге:
   - *каталог_сервера_bin*/dbbkapi/dsm.sys

   ```
   servername TSMDBMGR_TSMINST1
   commmethod         tcpip
   tcpserveraddr localhost
   tcpport           1500
   errorlogname /tsminst1/tsmdbmgr.log
   nodename $$_TSMDBMGR_$$
   ```

   где
   - *servername* соответствует значению `servername` в файле `tsmdbmgr.opt`.
   - *commethod* задает API клиента, используемый для связи с сервером при резервном копировании базы данных. Это может быть значение `tcpip` или `sharedmem`. Дополнительную информацию о совместно используемой памяти смотрите в описании шага 5.
   - *tcpserveraddr* задает адрес сервера, который API клиента будет использовать для связи с сервером для резервного копирования базы данных. Для резервного копирования базы данных надо задать значение `localhost`.
   - *tcpport* задает номер порта, который API клиента будет использовать для связи с сервером с целью резервного копирования базы данных. Значение `tcpport` должно быть значением, которое задано в файле опций сервера dsmserv.opt.
   - *errorlogname* задает журнал ошибок, в который API клиента будет записывать ошибки, происходящие при резервном копировании базы данных. Обычно этот журнал находится в каталоге экземпляра сервера. Однако его можно поместить в любой другой каталог, разрешения на запись в который есть у ID пользователя.
   - *nodename* задает имя узла, которое API клиента будет использовать для соединения с сервером при резервном копировании базы данных. Чтобы обеспечить возможность резервного копирования базы данных, нужно задать значение `$$_TSMDBMGR_$$`.
5. Необязательно: Сконфигурируйте сервер для резервного копирования базы данных с использованием совместно используемой памяти. Таким образом вы можете уменьшить нагрузку на процессор и увеличить пропускную способность. Сделайте следующее:
   a. Просмотрите файл dsmserv.opt. Если следующие строки отсутствуют в этом файле, то добавьте их:

      ```
      commmethod     sharedmem
      shmport номер_порта
      ```

      где *номер_порта* задает порт, используемый для совместно используемой памяти.
   b. В файле конфигурации dsm.sys найдите следующие строки:

      ```
      commmethod         tcpip
      tcpserveraddr localhost
      tcpport номер_порта
      ```

      Замените указанные строки следующими строками:

      ```
      commmethod     sharedmem
      shmport номер_порта
      ```

      где *номер_порта* задает порт, используемый для совместно используемой памяти.

AIX: Опции конфигурирования сервера для обслуживания сервера баз данных

Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

Об этой задаче

Для реорганизации таблиц и индексов требуются значительные процессорные ресурсы, пространство для активного журнала и пространство для архивного журнала. Поскольку резервное копирование баз данных имеет приоритет перед реорганизацией, выберите время и длительность для реорганизации так, чтобы эти процессы не перекрывались и реорганизация смогла завершиться.

 Операционные системы AIXВы можете оптимизировать реорганизацию индекса и таблиц для базы данных сервера. Таким образом можно избежать неожиданного роста базы данных и проблем, отрицательно влияющих на производительность. Инструкции смотрите в техническом примечании 1683633.

Если вы изменяете эти опции сервера при работающем сервере, надо остановить и перезапустить сервер, чтобы они вступили в силу.

Процедура

1. Измените опции сервера.
    Операционные системы AIXОтредактируйте файл опций сервера dsmserv.opt в каталоге экземпляра сервера. При изменении файла опций сервера придерживайтесь следующих рекомендаций:
   - Чтобы включить опцию, удалите звездочку в начале строки.
   - Введите опцию в любой строке.
   - Вводите по одной опции на строке. Вся опция со своим значением должна быть записана на одной строке.
   - Если для одной опции в файле есть несколько записей, сервер использует последнюю запись.

   Чтобы просмотреть доступные опции сервера, воспользуйтесь файлом примера dsmserv.opt.smp в каталоге /opt/tivoli/tsm/server/bin.
2. Если вы собираетесь использовать дедупликацию данных, то разрешите опцию сервера ALLOWREORGINDEX. Добавьте следующую опцию и значение в файл опций сервера:

   ```
   allowreorgindex yes
   ```

3. Задайте опции сервера REORGBEGINTIME и REORGDURATION, управляющие моментом начала реорганизации и ее длительностью. Выберите время и длительность, чтобы выполнять реорганизацию во время ожидаемой минимальной занятости сервера. Эти опции сервера действуют на процессы реорганизации как таблиц, так и индексов.
   a. Задайте время начала реорганизации при помощи опции сервера REORGBEGINTIME. Задайте время по 24-часовой системе. Например, чтобы начать реорганизацию в 8.30 вечера, задайте в файле опций сервера:

      ```
      reorgbegintime 20:30
      ```

   b. Задайте интервал, в который сервер может начать реорганизацию. Например, чтобы указать, что сервер может начать реорганизацию в течении четырех часов после времени, заданного опцией сервера REORGBEGINTIME, задайте в файле опций сервера:

      ```
      reorgduration 4
      ```

4. Если в момент изменения файла опций сервера сервер работает, остановите и перезапустите его.

 Операционные системы AIX

AIX: Запуск экземпляра сервера

Сервер можно запускать от имени ID пользователя экземпляра (что является предпочтительным методом) или от имени ID пользователя root.

Прежде чем начать

Убедитесь, что вы правильно задали разрешения и пределы пользователя.

 Операционные системы AIXИнструкции смотрите в разделе Проверка прав доступа и ограничений для пользователей.

Об этой задаче

При запуске сервера с использованием ID пользователя экземпляра упрощается процесс конфигурирования и исключаются потенциальные проблемы. Однако в некоторых случаях может потребоваться запуск сервера под ID пользователя root. Например, вы можете захотите использовать ID пользователя root, чтобы сервер мог обращаться к определенным устройствам. Можно настроить автоматический запуск сервера, используя либо ID пользователя экземпляра, либо ID пользователя root.

 Операционные системы AIXЕсли вам нужно выполнить задачи по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания.

Процедура

Чтобы запустить сервер, выполните одно из следующих действий:

- Запустите сервер от имени ID пользователя экземпляра.

   Операционные системы AIXИнструкции смотрите в разделе Запуск сервера от имени ID пользователя экземпляра.

- Запустите сервер от имени ID пользователя root.

  Инструкции по авторизации ID пользователей root для запуска сервера смотрите на веб-странице Авторизация ID пользователей root для запуска сервера (V7.1.1). Инструкции по запуску сервера с ID пользователя root смотрите на веб-странице Запуск сервера от имени ID пользователя root (V7.1.1).

-  Операционные системы AIXАвтоматический запуск сервера.

   Операционные системы AIXИнструкции смотрите в разделе AIX: Автоматический запуск серверов.

-  Операционные системы AIXЗапустите сервер в режиме обслуживания.

  Инструкции смотрите в разделе AIX: Запуск сервера в режиме обслуживания.

 Операционные системы AIX

AIX: Проверка прав доступа и ограничений для пользователей

Перед запуском сервера проверьте права доступа и пределы пользователя.

Об этой задаче

Если не проверить пользовательские пределы (другое название - *значения ulimit*, могут возникнуть нестабильность или ошибки ответов сервера. Нужно также проверить предел для максимального числа открытых файлов, установленный на уровне системы. Этот предел на уровне системы не может быть меньше пользовательского предела.

Процедура

1. Убедитесь, что у ID пользователя экземпляра сервера есть разрешения на запуск сервера.
2. Для экземпляра сервера, который вы собираетесь запускать, убедитесь, что у вас есть полномочия на чтение и запись файлов в каталоге этого экземпляра сервера. Проверьте, что в каталоге экземпляра сервера существует файл dsmserv.opt и он включает в себя параметры для экземпляра сервера.
3. Если сервер подключается к ленточному накопителю, чейнджеру носителей или устройству со сменными носителями, а вы собираетесь запускать сервер под ID пользователя экземпляра сервера, предоставьте этому ID пользователя доступ на чтение и запись для указанных устройств. Чтобы задать разрешения, выполните одно из следующих действий:
   - Если система выделена для IBM Spectrum Protect и доступ есть только у администратора IBM Spectrum Protect, задайте для специального файла устройства общий доступ с правом записи. Введите в командной строке операционной системы следующую команду:

     ```
     chmod +w /dev/rmtX
     ```

   - Если в системе несколько пользователей, вы можете ограничить доступ, сделав ID пользователя экземпляра IBM Spectrum Protect владельцем специальных файлов устройств. Введите в командной строке

операционной системы следующую команду:

```
chmod u+w /dev/rmtX
```

- Если на одном и том же компьютере работают экземпляры нескольких пользователей, измените имя группы, например, TAPEUSERS, и добавьте в эту группу каждый ID пользователя экземпляра IBM Spectrum Protect. Затем измените для специальных файлов устройств владельца, так чтобы их владельцем стала группа TAPEUSERS, и предоставьте группе разрешение на запись этих файлов. Введите в командной строке операционной системы следующую команду:

  ```
  chmod g+w /dev/rmtX
  ```

4. Проверьте следующие пределы пользователя на соответствие рекомендациям в таблице.

Табл. 1. Значения пользовательского предела (ulimit)

Тип пользовательского предела	**Рекомендуемое значение**	**Команда для запроса значения**
Максимальный размер создаваемых файлов ядра	Без ограничений	`ulimit -Hc`
Максимальный размер сегмента данных для процесса	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	65536	`ulimit -Hn`
Максимальное время процессора в секундах	Без ограничений	`ulimit -Ht`

Чтобы изменить пользовательские пределы, выполните инструкции в документации к используемой операционной системе.

Совет: Если вы собираетесь запускать сервер автоматически при помощи сценария, пользовательские пределы можно задать в этом сценарии.

5. Убедитесь, что для пользовательского предела максимального числа пользовательских процессов (`параметр nproc`) задано минимальное рекомендуемое значение 16384.
   a. Для проверки текущего пользовательского значения введите команду`ulimit -Hu` от имени ID пользователя экземпляра. Например:

   ```
   [user@Machine ~]$ ulimit -Hu
   16384
   ```

   b. Если предел максимального числа пользовательских процессов не равен 16384, то задайте значение 16384.
   Операционные системы AIXДобавьте следующую строку в файл /etc/security/limits:

   ```
   ID_пользователя_экземпляра        -     nproc           16384
   ```

   где *ID_пользователя_экземпляра* - это ID пользователя экземпляра сервера.

Операционные системы AIX

AIX: Запуск сервера от имени ID пользователя экземпляра

Чтобы запустить сервер под ID пользователя экземпляра, войдите в систему с ID пользователя root и введите в каталоге экземпляра сервера соответствующую команду.

Прежде чем начать

Убедитесь, что права доступа и пределы пользователей заданы правильно. Инструкции смотрите в разделе AIX: Проверка прав доступа и ограничений для пользователей.

Процедура

1. Войдите в систему, в которой установлен IBM Spectrum Protect, от имени ID пользователя экземпляра для сервера.
2. Если у вас нет профиля пользователя, который запускает сценарий `db2profile`, то введите следующую команду:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

Совет: Инструкции об изменении сценария входа в систему ID пользователя для автоматического запуска сценария `db2profile` смотрите в документации по DB2.

3. Запустите сервер, введя следующую команду в одной строке из каталога экземпляра сервера:

    Операционные системы AIX

   ```
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

    Операционные системы AIXНе забудьте поставить пробел после `SHMPSIZE=64K`. Запустив сервер с помощью этой команды, вы включаете для сервера страницы памяти по 64 КБ. Этот параметр поможет вам оптимизировать производительность сервера.

   Совет: Эта команда выполняется в режиме активного окна, так что вы сможете задать ID администратора и соединиться с экземпляром сервера.
    Операционные системы AIXНапример, если имя экземпляра сервера - `tsminst1`, а каталог экземпляра сервера - /tsminst1, введите следующие команды:

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

 Операционные системы AIX

AIX: Автоматический запуск серверов

Сервер можно сконфигурировать, так чтобы он запускался автоматически при запуске системы. Используйте специально предназначенный для этого сценарий rc.dsmserv.

Прежде чем начать

Убедитесь, что права доступа и пределы пользователей заданы правильно.

 Операционные системы AIXИнструкции смотрите в разделе Проверка прав доступа и ограничений для пользователей.

Об этой задаче

Сценарий rc.dsmserv находится в каталоге установки сервера, например, в каталоге /opt/tivoli/tsm/server/bin.

 Операционные системы AIXСовет: Если вы использовали мастер конфигурирования, то можно запускать сервер автоматически при перезапуске системы. При выборе этого варианта запись для запуска сервера добавляется автоматически в файл /etc/inittab.

Процедура

Если вы не использовали мастер для конфигурирования сервера, добавьте в файл /etc/inittab запись для каждого сервера, который вы хотите запускать автоматически:

1. Задайте в качестве уровня выполнения значение, соответствующее многопользовательскому режиму с включенной поддержкой работы по сети. Как правило, используется уровень выполнения 2, 3 или 5 в зависимости от операционной системы и ее конфигурации. Убедитесь, что уровень выполнения в файле /etc/inittab совпадает с уровнем выполнения операционной системы. Дополнительную информацию о многопользовательском режиме и уровнях выполнения смотрите в документации для используемой операционной системы.
2. Укажите в команде rc.dsmserv в файле /etc/inittab ID пользователя экземпляра при помощи опции -u и каталог экземпляра сервера при помощи опции -i. Если вы хотите запускать автоматически несколько экземпляров сервера, добавьте запись для каждого экземпляра сервера. Для проверки синтаксиса обратитесь к документации к операционной системе.
   Совет: Для автоматического запуска сервера под ID пользователя root используйте опцию -U.

Пример

Например, если имя владельца экземпляра - tsminst1, а каталог экземпляра сервера - /home/tsminst1/tsminst1, добавьте в /etc/inittab следующую запись (в виде одной строки):

Операционные системы AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```

В этом примере ID процесса - `tsm1`, а в качестве уровня выполнения задано значение 2.

Если у вас имеется несколько экземпляров сервера, которые вы хотите запускать, добавьте запись для каждого экземпляра сервера. Например, если у вас есть ID пользователей-владельцев экземпляров tsminst1 и tsminst2 и каталоги экземпляров /home/tsminst1/tsminst1 и /home/tsminst2/tsminst2, добавьте в /etc/inittab показанные ниже записи. Каждая запись должна находиться на одной строке.

Операционные системы AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
   -i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

Информация, связанная с данной:
Сценарий запуска сервера: rc.dsmserv
Операционные системы AIX

AIX: Запуск сервера в режиме обслуживания

Сервер можно запустить в режиме обслуживания, чтобы избежать повреждений при выполнении задач по обслуживанию и переконфигурированию.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

   ```
   halt
   ```

2. Запустите сервер, используя метод, который вы используете в производственном режиме.

Операции, которые были отключены во время режима обслуживания, будут снова включены.

AIX: Остановка сервера

При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.

Об этой задаче

Чтобы остановить сервер, введите в командной строке IBM Spectrum Protect следующую команду:

```
halt
```

 Операционные системы AIXЕсли невозможно подключиться к серверу в качестве клиента администрирования, но нужно остановить сервер, следует отменить процесс с помощью команды kill с указанием идентификационного номера (pid) процесса. Значение pid будет показано при инициализации.
Важное замечание: Перед тем, как ввести команду kill, убедитесь что вам известен правильный идентификатор сервера IBM Spectrum Protect.
Для определения номера процесса, который нужно выгрузить, можно использовать файл `dsmserv.v6lock` в том каталоге, из которого запущен сервер. Чтобы увидеть файл, введите:

```
cat /instance_dir/dsmserv.v6lock
```

 Операционные системы AIXЧтобы остановить сервер, введите следующую команду:

```
kill -36 dsmserv_pid
```

где *dsmserv_pid* - это числовой ID процесса.

AIX: Регистрация лицензий

Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.

Об этой задаче

Используйте для этого команду REGISTER LICENSE. Дополнительные сведения смотрите в разделе REGISTER LICENSE.

Пример: Зарегистрировать лицензию

Зарегистрируйте базовую лицензию на IBM Spectrum Protect.

```
register license file=tsmbasic.lic
```

AIX: Подготовка сервера к операциям резервного копирования базы данных

Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.

Процедура

1. Убедитесь, что конфигурация IBM Spectrum Protect - полная. Если вы не используете мастер конфигурирования (dsmicfgx) для конфигурирования сервера, убедитесь, что вы выполнили шаги по конфигурированию сервера вручную для резервного копирования базы данных.
2. Выберите класс устройств, который следует использовать для резервного копирования базы данных, защитите главный ключ шифрования и задайте пароль. Все эти действия выполняются путем ввода команды SET DBRECOVERY из административной командной строки:

```
set dbrecovery имя_класса_устройств protectkeys=yes password=имя_пароля
```

где *имя_класса_устройств* задает класс устройств, который следует использовать для операций резервного копирования базы данных, а *имя_пароля* задает пароль.
Вы обязательно должны задать имя класса устройств, иначе резервное копирование завершится неудачно. Задав PROTECTKEYS=YES, вы сделаете так, что во время операций резервного копирования базы данных будет создаваться резервная копия главного ключа шифрования.
Важное замечание: Создайте надежный пароль, содержащий хотя бы 8 символов. Убедитесь, что вы запомнили этот пароль. Если задан пароль для резервной копии базы данных, вы должны указать тот же самый пароль в команде RESTORE DB для восстановления базы данных.

Пример

Чтобы указать, что резервные копии базы данных содержат копию главного ключа шифрования для сервера, введите следующую команду:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

AIX: Запуск нескольких экземпляров серверов на одном компьютере

Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.

Умножьте требования к памяти и другим системным ресурсам для одного сервера на число экземпляров, которые вы собираетесь создать в системе.

 Операционные системы AIXНабор файлов для одного экземпляра сервера хранится отдельно от файлов, используемым другим экземпляром сервера в той же системе. Выполните для каждого нового экземпляра шаги, описанные в разделе AIX: Создание экземпляра сервера, включая создание пользователя нового экземпляра.

Чтобы управлять объемом системной памяти, используемым каждым сервером, задайте опцию DBMEMPERCENT, позволяющую ограничить процент системной памяти. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.

Можно произвести обновление V7.1 до V8.1 напрямую. Более подробную информацию смотрите в разделе об обновлении (Обновление до V8.1). Если при обновлении в вашей системе есть несколько серверов, запускать мастер установки нужно только один раз. Мастер установки соберет информацию о базах данных и переменных для всех исходных экземпляров сервера.

Если вы выполняете обновление IBM Spectrum Protect V6.3 до V8.1.5 и в системе есть несколько серверов, то все экземпляры, существующие в DB2 V9.7, удаляются и заново создаются в DB2 V11.1. Мастер сгенерирует команду `db2 upgrade db имя_бд` для каждой базы данных. В процессе обновления также будет произведено переконфигурирование переменных среды базы данных для каждого экземпляра в вашей системе.

Задачи, связанные с данной:
Запуск нескольких экземпляров серверов на одном компьютере (V7.1.1)

AIX: Мониторинг сервера

Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Процедура

1. Следите за активным журналом, чтобы убедиться, что его размер соответствует рабочей нагрузке, обрабатываемой экземпляром сервера.

   Если уровень рабочей нагрузки на сервер приближается к типичному ожидаемому уровню, то объем пространства, используемого активным журналом, составляет 80-90% пространства. В этот момент, возможно, нужно увеличить объем пространства. Необходимость увеличения пространства зависит от типов транзакций, составляющих

рабочую нагрузку сервера. Характеристики транзакций влияют на то, как используется пространство активного журнала.

На использованием пространства активного журнала могут влиять следующие характеристики транзакций:

- Число и размер файлов в операциях резервного копирования.
  - Такие клиенты, как файл-серверы, которые создают резервные копии большого числа мелких файлов, могут инициировать большое число быстро завершающихся транзакций. Транзакции могут использовать большой объем пространства в активном журнале, но кратковременно.
  - Такие клиенты, как почтовый сервер или сервер базы данных, которые создают резервные копии больших объемов данных в ходе немногочисленных транзакций, могут инициировать небольшое число транзакций, для завершения которых требуется длительное время. Транзакции могут использовать небольшой объем пространства в активном журнале, но в течение длительного времени.
- Типы соединений с сетью
  - Транзакции, связанные с операциями резервного копирования, которые выполняются с использованием высокоскоростных сетевых соединений, завершаются быстрее. Транзакции используют пространство в активном журнале в течение более короткого времени.
  - Для завершения транзакций, связанных с операциями резервного копирования, которые выполняются с использованием относительно низкоскоростных сетевых соединений, требуется больше времени. Транзакции используют пространство в активном журнале в течение более длительного времени.

Если сервер обрабатывает транзакции с широким диапазоном характеристик, то пространство, используемое для активного журнала, может значительно увеличиваться и уменьшаться с течением времени. В этом случае вы должны сделать так, чтобы, как правило, использовался меньший процент пространства активного журнала. Дополнительное пространство позволит активному журналу увеличиваться в размере, если для выполнения транзакций требуется очень много времени.

2. Следите за архивным журналом, чтобы убедиться в том, что для него всегда хватает места.
   Напоминание: Если архивный журнал и архивный журнал отказоустойчивости заполнятся, может заполниться активный журнал, и сервер остановится. Цель заключается в том, чтобы архивному журналу был доступен достаточный объем пространства и он никогда не использовал все доступное ему пространство.
   Вы, вероятно, заметите следующие закономерности:
   a. Сначала архивный журнал быстро растет по мере выполнения операций резервного копирования клиента.
   b. Резервное копирование базы данных производится регулярно либо по расписанию, либо вручную.
   c. После выполнения, как минимум, двух операций полного резервного копирования базы данных сокращение журналов происходит автоматически. В результате отбрасывания пространство, используемое архивным журналом, уменьшается.
   d. Обычные операции клиента продолжаются, и архивный журнал снова растет.
   e. Резервное копирование базы данных выполняется регулярно, и отбрасывание журналов происходит так же часто, как и операции полного резервного копирования базы данных.

   При таких закономерностях архивный журнал сначала растет, затем уменьшается, а затем может снова вырасти. С течением времени, по мере продолжения нормальной работы, объем пространства, используемого архивным журналом, должен достичь относительно постоянного уровня.

   Если архивный журнал продолжает расти, то выполните одно из описанных ниже действий или оба эти действия:
   - Добавьте пространство для архивного журнала. Это может означать перемещение архивного журнала в другую файловую систему.
   - Увеличьте частоту полного резервного копирования базы данных, чтобы отбрасывание журналов производилось чаще.
3. Если вы задали каталог для резервного архивного журнала, определите, сохраняются ли в этом каталоге какие-либо журналы при обычной работе. Если пространство резервного журнала используется, то увеличьте размер архивного журнала. Цель состоит в том, чтобы резервный архивный журнал использовался только в экстраординарных условиях, а не при обычной работе.

AIX: Установка пакета исправлений сервера IBM Spectrum Protect

Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.

Прежде чем начать

Чтобы установить на сервер пакет Fix Pack или промежуточный пакет исправлений, установите сервер требуемого для выполнения уровня. Не обязательно запускать установку сервера на уровне базового выпуска. Например, если у вас установлена версия 8.1.1, то можно перейти сразу к самому последнему пакету Fix Pack для V8.1. Не обязательно начинать с установки V8.1.0, если доступно текущее изменение.

У вас должен быть установлен пакет лицензий IBM Spectrum Protect. Пакет лицензий приобретается вместе с базовым выпуском программного обеспечения. При загрузке пакета исправлений или промежуточного пакета исправлений с сайта Fix Central установите лицензию на сервер, которая есть на веб-сайте Passport Advantage. Для вывода сообщений и справки на языке, ином чем американский английский, установите языковый пакет по своему выбору.

Если вы обновляете сервер до V8.1.5 или новее, а затем возвращаетесь к уровню сервера, более раннему, чем V8.1.5, необходимо восстановить базу данных на момент времени, предшествующий обновлению. Во время процесса обновления выполните требуемые действия, обеспечивающие возможность восстановления базы данных: создайте резервные копии базы данных, файла хронологии тома, файла конфигурации устройств и файла опций сервера. Дополнительные сведения смотрите в разделе AIX: Возврат от версии 8.1.5 к предыдущему серверу.

Если вы используете службу управления клиентами, убедитесь, что вы обновили ее до той же версии, к которой относится сервер IBM Spectrum Protect.

Убедитесь, что вы сохранили установочный носитель базового выпуска установленного сервера. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.

Посетите страницу Портал поддержки IBM® и найдите там следующую информацию:

- Список последних исправлений и их скачивание. Щелкните по **Downloads** (Материалы для скачивания) и примените все соответствующие исправления.
- Подробности получения базового пакета лицензий. Найдите **Downloads > Passport Advantage** (Материалы для скачивания - Passport Advantage).
- Поддерживаемые платформы и системные требования. Укажите для поиска: **поддерживаемые операционные системы IBM Spectrum Protect**.

Обязательно обновите сервер, прежде чем обновлять клиенты резервного копирования и архивирования. Если не обновить сначала сервер, связь между серевром и клиентами может прерваться.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

Процедура

Чтобы установить пакет исправлений или промежуточное исправление, сделайте следующее:

1. Создайте резервную копию базы данных. Рекомендуется способ использовать резервное копирование в режиме снимка. Резервное копирование в режима снимка - это полное резервное копирование базы данных, не прерывающее никаких плановых операций резервного копирования базы данных. Например, введите следующую команду управления IBM Spectrum Protect:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте резервную копию информации о конфигурации устройств. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup devconfig filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
3. Сохраните файл хронологии томов в другом положении или переименуйте этот файл. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt. Этот файл расположен в каталоге экземпляра сервера.

5. Прежде чем устанавливать пакет исправлений или промежуточное исправление, остановите сервер. Используйте команду HALT.
6. Убедитесь, что в каталоге установки доступно дополнительное пространство. Установка этого пакета Fix Pack может потребовать дополнительного временного дискового пространства в каталоге установки сервера. Объем дополнительного дискового пространства может быть таким же, как требуется для установки новой базы данных как части установки IBM Spectrum Protect. Мастер по установке IBM Spectrum Protect показывает объем пространства, требуемого для установки пакета Fix Pack, и доступный объем пространства. Если требуемый объем пространства превышает доступный, установка прекращается. Если установка остановилась, добавьте требуемое дисковое пространство к файловой системе и перезапустите установку.
7.  Операционные системы AIXВойдите в систему от имени пользователя root.
8. Получите файл пакета исправлений или промежуточного исправления, который вы хотите установить, со страниц Портал поддержки IBM, Passport Advantage или Fix Central.
9.  Операционные системы AIXПерейдите в каталог, куда вы поместили выполняемый файл, и сделайте следующее.
   Совет: Файлы извлекаются в текущий каталог. Убедитесь, что исполняемый файл находится в каталоге, куда будут извлекаться файлы.
   a. Измените разрешения на доступ к файлам, введя следующую команду:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-платформа.bin
      ```

      где *платформа* - это архитектура, в которой устанавливается IBM Spectrum Protect.
   b. Чтобы извлечь файлы установки, введите следующую команду:

      ```
      ./8.x.x.x-IBM-SPSRV-платформа.bin
      ```

10. Выберите один из следующих способов установки IBM Spectrum Protect.
    Важное замечание: После установки пакета исправлений не нужно снова выполнять все шаги по конфигурированию. Вы можете остановить программу после завершения установки, исправить все ошибки и перезапустить свои серверы.
    Установите программное обеспечение IBM Spectrum Protect одним из следующих способов:

    Мастер установки
    : Выполните инструкции для вашей операционной системы.
      AIX: Установка IBM Spectrum Protect при помощи мастера установки

    Совет: Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.

    Командная строка в режиме консоли
    : Выполните инструкции для вашей операционной системы.
      AIX: Установка IBM Spectrum Protect в режиме консоли

    Режим без вывода сообщений
    : Выполните инструкции для вашей операционной системы.
      AIX: Установка IBM Spectrum Protect в режиме без вывода сообщений

    Совет: Если в вашей системе используется несколько экземпляров сервера, запустите мастер установки только один раз. Мастер по установке обновит все экземпляры сервера.

Результаты

Исправьте ошибки, обнаруженные в процессе установки.

Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по Файл > Просмотреть журнал. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по Справка > Экспорт данных для анализа ошибок.

Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:

-  Операционные системы AIX/var/ibm/InstallationManager/logs
-  Операционные системы AIXAIX: Применение пакета Fix Pack к IBM Spectrum Protect V8.1.5 в кластерной среде для AIX
  Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень. Пакет исправлений можно применить в кластерной среде для AIX.

AIX: Возврат от версии 8.1.5 к предыдущему серверу

Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.

Прежде чем начать

У вас должны быть следующие элементы для более ранней версии сервера:

- Резервная копия базы данных сервера
- Файл хронологии тома
- Файл конфигурации устройств
- Файл серверных опций

Об этой задаче

Используйте одни и те же инструкции и для возврата к прежней версии в пределах одного выпуска (например, от 8.1.3 до 8.1.2 или от 8.1.3 до 7.1.2). Прежняя версия должна совпадать с версией, использовавшейся перед обновлением до версии 8.1.

Внимание: Задайте значение параметра REUSEDELAY, помогающее предотвратить потерю данных клиента резервного копирования и архивирования при возврате сервера к прежней версии.

Шаги по возврату к предыдущей версии сервера

Об этой задаче

Выполните следующие действия в системе, где установлен сервер версии 8.1:

Процедура

1. Остановите сервер, чтобы закрыть все операции сервера, с помощью команды HALT.
2. Удалите базу данных из менеджера базы данных, затем удалите каталоги базы данных и журналов восстановления.
   a. Вручную удалите базу данных. Один из способов удалить ее - ввести следующую команду:
    Операционные системы AIX

   ```
   dsmserv removedb tsmdb1
   ```

   b. Если вам нужно снова использовать пространство, занятое каталогами базы данных и журналов восстановления, вы теперь можете удалить эти каталоги.
3. Деинсталлируйте сервер V8.1 при помощи программы деинсталляции. При деинсталляции удаляется сервер и менеджер баз данных вместе с их каталогами. Дополнительные сведения смотрите в разделе AIX: Деинсталляция IBM Spectrum Protect.
4. Остановите службу кластеров. Заново установите версию программы сервера, которую вы использовали перед обновлением до V8.1.5. Эта версия должна совпадать с версией вашего сервера на момент создания резервной копии базы данных, которую вы восстановите в одном из последующих шагов. Например, перед обновлением сервер относился к версии 7.1.7, а вы собираетесь применить резервную копию базы данных, использовавшуюся на этом сервере. Чтобы получить возможность восстанавливать эту резервную копию базы данных, нужно установить Fix Pack для V7.1.7.
5. Сконфигурируйте новую базу данных сервера при помощи мастера конфигурирования. Чтобы запустить мастер, введите следующую команду:  Операционные системы AIX

   ```
   . /dsmicfgx
   ```

6. Убедитесь, что нет серверов, запущенных в фоновом режиме.
7. Восстановите базу данных на заданный момент времени перед обновлением.
8. Скопируйте следующие файлы в каталог экземпляра.
   - Файл конфигурации устройств
   - Файл хронологии тома
   - Файл опций сервера (обычно, dsmserv.opt)

9. Если вы включили дедупликацию данных для каких-либо пулов хранения типа FILE, которые существовали перед обновлением, или если вы при использовании сервера V8.1.5 перенесли данные, существовавшие перед обновлением, в новые пулы хранения, вы должны будете выполнить дополнительные шаги по восстановлению. Дополнительные сведения смотрите в разделе Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных.
10. Если значение параметра REUSEDELAY для пулов хранения меньше возраста восстанавливаемой вами базы данных, восстановите тома во всех пулах хранения с последовательным доступом, которые были консолидированы после резервного копирования базы данных. Используйте команду RESTORE VOLUME.
    Если у вас нет резервной копии пула хранения, произведите аудит консолидированных томов при помощи команды AUDIT VOLUME с параметром FIX=YES для устранения противоречий. Например:

    ```
    audit volume имя_тома fix=yes
    ```

11. Если с использованием сервера версии 8.1 выполнялись операции резервного копирования или архивирования клиента, выполните аудит томов пулов хранения, на которых были сохранены эти данные.

Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных

Если во время работы сервера в версии 8.1.5 вы создавали новые пулы хранения, включали дедупликацию данных для любых пулов хранения типа FILE или совершали оба этих действия, необходимо выполнить некоторые дополнительные шаги, чтобы вернуться к предыдущей версии сервера.

Прежде чем начать

Чтобы вы смогли выполнить эту задачу, у вас должна быть полная резервная копия пула хранения, созданная до обновления до версии 8.1.5.

Об этой задаче

Используйте приведенную ниже информацию, если какое-то время у вас работал сервер V8.1.5 и вы в это время выполняли любое из следующих действий (или оба эти действия):

- Вы включили функцию дедупликации данных для любых пулов хранения, которые существовали до обновления до программы версии 8.1.5. Дедупликация данных применима только к пулам хранения, в которых используется тип устройств FILE.
- После обновления вы создали новые первичные пулы хранения *и* перенесли в эти новые пулы хранения данные, хранившиеся в других пулах хранения.

Выполните описанные ниже шаги после восстановления сервера до V7.

Процедура

- Для каждого пула хранения, для которого вы включили функцию дедупликации данных, восстановите весь пул хранения при помощи команды RESTORE STGPOOL.
- Для пулов хранения, созданных после обновления, определите, какие действия вам следует предпринять. Данные, перенесенные из существующих пулов хранения V8 в новые пулы хранения, могут быть потеряны, так как на восстановленном сервере V8 этих новых пулов не будет. Возможный способ выхода из этой ситуации зависит от типа пула хранения:
  - Если данные были перенесены в новый пул хранения из пулов хранения типа DISK, относящихся к V8, пространство, которое занимали перенесенные данные, вероятнее всего, было уже использовано повторно. Поэтому вы должны будете восстановить исходные пулы хранения V8, используя резервные копии этого пула хранения, созданные перед обновлением до V8.1.5.

    Если в новый пул хранения *не* переносились никакие данные из пулов хранения типа DISK, относящихся к V8, то произведите аудит томов пула хранения в этих пулах хранения типа DISK.

  - Если данные были перенесены в новый пул хранения из пулов хранения с последовательным доступом, относящихся к V8, эти данные могут все еще существовать на томах пула хранения на восстановленном сервере V8 и быть пригодны для использования. Эти данные, вероятнее всего, будут пригодны для использования, если для параметра REUSEDELAY для этого пула хранения было задано значение, не позволившее произвести в нем консолидацию пространства, когда сервер работал как сервер V8.1.5. Если

какие-либо тома были подвергнуты консолидации, когда сервер работал как сервер Версии 8.1.5, эти тома нужно будет восстановить из резервных копий пула хранения, созданных перед обновлением до V8.1.5.

AIX: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect

Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.

Назначение

Иногда после использования мастеров по установке и конфигурированию IBM Spectrum Protect вам потребуется ввести команды DB2. Ограниченный набор команд DB2, которые вы можете использовать (в частности, по указанию службы поддержки), представлен в списке в Табл. 1. Это не исчерпывающий список, он представлен только в виде дополнительного материала. Не предполагается, что администратор IBM Spectrum Protect будет ежедневно или вообще регулярно использовать эти команды. Приведены примеры использования некоторых команд. Подробности выходной информации не представлены.

Полное объяснение описанных здесь команд и их синтаксиса смотрите в Информационном центре Информация о DB2.

Табл. 1. Команды DB2

Команда	**Описание**	**Пример**
db2icrt	Создает экземпляры DB2 в домашнем каталоге владельца экземпляра. Совет: Мастер по конфигурированию IBM Spectrum Protect создает экземпляр, используемый сервером и базой данных. После того, как сервер установлен и сконфигурирован с помощью мастера по конфигурированию, команда db2icrt обычно не используется. Операционные системы AIXЭта утилита находится в каталоге DB2DIR/instance, где DB2DIR представляет собой положение установки текущей версии системы баз данных DB2.	Создайте экземпляр IBM Spectrum Protect вручную.Введите команду в одной строке: `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`имя_экземпляра имя_экземпляра`*
db2set	Выводит переменные DB2.	Вывести список переменных DB2: `db2set`
CATALOG DATABASE	Сохраняет информацию о положении базы данных в системном каталоге баз данных. База данных может находиться или на локальной рабочей станции, или на удаленном сервере разделов базы данных. Мастер по конфигурированию серверов учитывает все каталоги, которые нужны для использования базы данных сервера. После того, как сервер сконфигурирован и запущен, вручную запустите эту команду, только если что-то в среде изменяется или повреждено.	Каталогизируйте базу данных: `db2 catalog database tsmdb1`

Команда	Описание	Пример
CONNECT TO DATABASE	Соединяется с заданной базой данных для использования интерфейса командной строки (command-line interface, CLI).	Соединитесь с базой данных IBM Spectrum Protect в интерфейсе командной строки DB2: `db2 connect to tsmdb1`

GET DATABASE CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Показать информацию конфигурации для алиаса базы данных:
		`db2 get db cfg for tsmdb1`
		Получить информацию для проверки параметров конфигурации базы данных, режима журналов и техобслуживания.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Получить информацию конфигурации для менеджера баз данных: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Получает информацию о состоянии работоспособности для менеджера баз данных и его баз данных. Возвращаемая информация представляет снимок состояния работоспособности на момент ввода команды. IBM Spectrum Protect отслеживает состояние базы данных при помощи снимка работоспособности и других механизмов, представленных DB2. Может так случиться, что снимок работоспособности или другой инструмент документации DB2 свидетельствует о возможном состоянии оповещения некоторого элемента или ресурса базы данных. Это означает, что нужно принять меры для исправления ситуации. IBM Spectrum Protect отслеживает условия и отвечает соответствующим образом. Обрабатываются не все выявленные оповещения DB2.	Получить отчет об индикаторах отслеживания работоспособности DB2: `db2 get health snapshot for database on tsmdb1`

Команда	Описание	Пример

GRANT (Полномочия базы данных)	Предоставляет полномочия, применимые ко всей базе данных, в отличие от привилегий, применимых к конкретным объектам в базе данных.	Предоставить доступ для ID пользователя itmuser:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Изменяет статистику, относящуюся к характеристикам таблицы и связанных индексов, или статистические производные таблицы. Эти характеристики включают в себя количество записей, количество страниц и среднюю длину записи. Запустите эту утилиту, чтобы увидеть таблицу после ее изменения или реорганизации. Производная таблица должна быть включена для оптимизации, чтобы ее можно было использовать для оптимизации запросов. Включенная для оптимизации производная таблица называется статистической производной таблицей. Используйте оператор DB2 ALTER VIEW , чтобы включить производную таблицу для оптимизации. Запустите утилиту RUNSTATS, когда изменения в рассматриваемых таблицах существенно влияют на возвращаемые в производной таблице строки. Совет: Сервер конфигурирует DB2 для запуска при необходимости команды RUNSTATS.	Изменить статистику для одной таблицы. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SETSCHEMA	Изменяет значение специального регистра CURRENT SCHEMA, подготавливаясь к вводу команд SQL непосредственно через интерфейс командной строки DB2. Совет: Специальный регистр - это область хранения, определенная для процесса применения менеджером баз данных. Он используется для хранения информации, на которую могут ссылаться операторы SQL.	Задать схему для IBM Spectrum Protect: `db2 set schema tsmdb1`
STARTDATABASEMANAGER	Запускает фоновые процессы текущего экземпляра менеджера баз данных. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Запустить менеджер баз данных: `db2start`

Команда	Описание	Пример
STOP DATABASE MANAGER	Останавливает текущий экземпляр менеджера баз данных. Менеджер баз данных остается активным, пока он не остановлен явным образом. Эта команда не останавливает экземпляр менеджера баз данных, если какие-либо приложения соединены с базами данных. Если соединений с базой данных нет, но есть подключения экземпляра, эти подключения экземпляра первыми принудительно прерываются данной командой. Затем она останавливает менеджер баз данных. Перед остановкой менеджера баз данных эта команда деактивирует также все невыполненные обращения к базе данных. Для клиента эта команда недопустима. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Остановить менеджер баз данных: `db2 stop dbm`

AIX: Деинсталляция IBM Spectrum Protect

Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Прежде чем начать

Прежде чем деинсталлировать IBM Spectrum Protect, выполните следующие шаги:

- Выполните полное резервное копирование базы данных.
- Сохраните копию хронологии томов и файлов конфигурации устройств.
- Поместите полученные тома в надежное место.

Об этой задаче

IBM Spectrum Protect можно деинсталлировать любым из следующих способов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

- AIX: Деинсталляция IBM Spectrum Protect при помощи графического мастера
  IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.
- AIX: Деинсталляция IBM Spectrum Protect в режиме консоли
  Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.
- AIX: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений
  Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.
- AIX: Деинсталляция и переустановка IBM Spectrum Protect
  Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.
- AIX: Деинсталляция IBM Installation Manager
  Можно деинсталлировать IBM Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Дальнейшие действия

Информацию о том, какие шаги по установке нужно выполнить, чтобы переустановить компоненты IBM Spectrum Protect, смотрите в разделе AIX: Установка компонентов сервера.

AIX: Деинсталляция IBM Spectrum Protect при помощи графического мастера

IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.

Процедура

1. Запустите Installation Manager.
    Операционные системы AIXВ каталоге, в котором установлен Installation Manager, перейдите в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду:

   ```
   ./IBMIM
   ```

2. Щелкните по Деинсталлировать.
3. Выберите Сервер IBM Spectrum Protect и щелкните по Далее.
4. Щелкните по Деинсталлировать.
5. Щелкните по Готово.

AIX: Деинсталляция IBM Spectrum Protect в режиме консоли

Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   -  Операционные системы AIXeclipse/tools

   Например:

   -  Операционные системы AIX/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду:
   -  Операционные системы AIX`./imcl -c`
3. Для деинсталляции введите `5`.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите `N` (Next - Далее).
6. Выберите деинсталляцию пакета сервера IBM Spectrum Protect.
7. Введите `N` (Next - Далее).
8. Введите `U` (Uninstall - Деинсталляция).
9. Введите `F` (Finish - Готово).

AIX: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений

Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции компонентов сервера IBM Spectrum Protect в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, uninstall_response_sample.xml, в каталоге input в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Если вы хотите деинсталлировать все компоненты IBM Spectrum Protect, оставьте заданное значение `modify="false"` для каждого компонента в файле ответов. Если вы не хотите деинсталлировать компонент, задайте значение `modify="true"`.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы AIXeclipse/tools

   Например:

   - Операционные системы AIX/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду, где *файл_ответов* - это полное имя файла ответов:
   Операционные системы AIX

   ```
   ./imcl -input файл_ответов -silent
   ```

   Пример команды:

   Операционные системы AIX

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

AIX: Деинсталляция и переустановка IBM Spectrum Protect

Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.

Об этой задаче

Чтобы вручную деинсталлировать и переустановить IBM Spectrum Protect, выполните следующие шаги:

1. Операционные системы AIXПрежде чем приступать к деинсталляции, создайте список текущих экземпляров сервера. Введите команду:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Введите для каждого экземпляра сервера следующую команду:
   Операционные системы AIX

   ```
   db2 attach to имя_экземпляра
   db2 get dbm cfg show detail
   db2 detach
   ```

   Запишите путь базы данных для каждого экземпляра.
3. Деинсталлируйте IBM Spectrum Protect. Смотрите раздел AIX: Деинсталляция IBM Spectrum Protect.
4. При деинсталляции любой поддерживаемой версии IBM Spectrum Protect, включая пакет исправлений, создается файл экземпляра. Файл экземпляра создается для того, чтобы помочь вам переустановить IBM Spectrum Protect. Проверьте этот файл и используйте эту информацию, когда вас попросят ввести идентификационные данные экземпляра при переустановке. При установке в режиме без вывода сообщений вы предоставляете эти идентификационные данные при помощи переменной `INSTANCE_CRED`.
   Положение файла экземпляра:
   - Операционные системы AIX/etc/tivoli/tsm/instanceList.obj
5. Переустановите IBM Spectrum Protect. Смотрите раздел AIX: Установка компонентов сервера.

   Если файл `instanceList.obj` не существует, вы должны заново создать экземпляры сервера, используя следующие шаги:

   a. Заново создайте экземпляры сервера. Смотрите раздел AIX: Создание экземпляра сервера.
      Совет: Мастер установки сконфигурирует экземпляры сервера, но вы должны убедиться, что они существуют. Если они не существуют, вы должны будете сконфигурировать их вручную.
   b. Каталогизируйте базу данных. Поочередно войдите в систему от имени пользователя экземпляра для каждого экземпляра сервера и введите следующие команды:
      Операционные системы AIX

```
db2 catalog database tsmdb1
db2 attach to имя_экземпляра
db2 update dbm cfg using dftdbpath каталог_экземпляра
db2 detach
```

c. Операционные системы AIXУбедитесь, что экземпляр сервера создан успешно.Введите команду:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

d. Убедитесь, что IBM Spectrum Protect распознает экземпляры сервера, вызвав спи сок ваших каталогов. Вы увидите ваш домашний каталог (если вы его не изменили). Если вы использовали мастер конфигурирования, ваш каталог экземпляра не появится. Введите команду:

```
db2 list database directory
```

Если вы увидите в списке TSMDB1, вы можете запустить сервер.

AIX: Деинсталляция IBM Installation Manager

Можно деинсталлировать IBM® Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Прежде чем начать

Перед удалением IBM Installation Manager, необходимо убедиться, что все пакеты, установленные IBM Installation Manager, удалены. Закройте IBM Installation Manager перед запуском деинсталляции.

Операционные системы AIXДля просмотра установленных пакетов введите следующую команду в командной строке:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Процедура

Чтобы деинсталлировать IBM Installation Manager, выполните следующие шаги:

Операционные системы AIX

1. Откройте командную строку и перейдите в каталог /var/ibm/InstallationManager/uninstall.
2. Введите следующую команду:

   ```
   ./uninstall
   ```

   Ограничение: Вы должны войти в систему от имени ID пользователя `root`.

Linux: Установка сервера

Установка сервера включает в себя планирование, установку и первоначальное конфигурирование.

- Linux: Планирование установки сервера
  Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.
- Linux: Установка компонентов сервера
  Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.
- Linux: Первые шаги после установки IBM Spectrum Protect
  После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.
- Linux: Установка пакета исправлений сервера IBM Spectrum Protect
  Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.
- Linux: Возврат от версии 8.1.5 к предыдущему серверу
  Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые

файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.
- Linux: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect
  Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.
- Linux: Деинсталляция IBM Spectrum Protect
  Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Linux: Планирование установки сервера

Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.

- Linux: Что нужно знать в первую очередь
  Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.
- Linux: Планирование для достижения оптимальной производительности
  Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.
- Операционные системы LinuxLinux: Минимальные требования к системе для систем Linux
  Чтобы установить сервер IBM Spectrum Protect в системе Linux, требуется минимальный уровень аппаратного и программного обеспечения, включая способ связи и самую последнюю версию драйверов устройств.
- Операционные системы LinuxLinux: Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе
  При определенных ограничениях на одном компьютере с сервером IBM Spectrum Protect версии 8.1.5 можно установить другие продукты, которые тоже внедряют и используют DB2.
- Linux: IBM Installation Manager
  IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.
- Linux: Контрольные списки для планирования сведений о сервере
  Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.
- Linux: Планирование мощностей
  Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.
- Linux: Практические рекомендации по именованию сервера
  Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.
- Linux: Каталоги установки
  К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

Linux: Что нужно знать в первую очередь

Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.

Выпуски пакетов сервисного обслуживания сервера, программное обеспечение клиента и публикации есть по адресу: Портал поддержки IBM®.

 Операционные системы LinuxОграничение: Можно установить и запустить версию 8.1.5сервера в системе, где уже установлена DB2, причем DB2 могла быть установлена независимо или как часть другой прикладной программы, хотя существуют некоторые ограничения. Чтобы узнать об этом подробнее, смотрите раздел, посвященный совместимости с другими продуктами DB2.

Опытные администраторы DB2 смогут выполнять сложные запросы SQL и использовать инструменты DB2 для мониторинга базы данных. Однако не следует использовать инструменты DB2 ни для изменения параметров конфигурации DB2, предварительно заданных IBM Spectrum Protect, ни для модификации среды DB2 для IBM Spectrum

Protect какими-либо другими способами (как это допускается при работе с другими продуктами). Сервер V8.1.5 построен и подвергнут расширенному тестированию с использованием языка определений данных (Data Definition Language - DDL) и конфигурации базы данных, которые внедряет сервер.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

Linux: Планирование для достижения оптимальной производительности

Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.

Процедура

1. Ознакомьтесь с разделом Linux: Что нужно знать в первую очередь.
2. Прочтите каждый из следующих подразделов.

- Linux: Планирование оборудования и операционной системы сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Linux: Планирование для дисков базы данных сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Linux: Планирование для дисков журнала восстановления сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Linux: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров
  Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.
- Linux: Планирование для пулов хранения на устройствах классов устройств DISK или FILE
  Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.
- Linux: Планирование правильного типа технологии хранения
  У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.
- Linux: Применение наилучших практических методов к установке сервера
  Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Linux: Планирование оборудования и операционной системы сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Соответствуют ли операционная система и оборудование требованиям или превышают их? • Число и частота процессоров • Системная память • Поддерживаемый уровень операционной системы	Если вы используете минимально необходимый объем памяти, вы можете поддерживать минимальную рабочую нагрузку. Вы можете поэкспериментировать, добавляя больше системной памяти, чтобы определить, повышается ли производительность. Затем решите, хотите ли вы оставить системную память выделенной для сервера. Проверьте различные вариации памяти, используя весь ежедневный цикл рабочей нагрузки сервера. Если у вас в системе работает несколько серверов, прибавьте требования для каждого сервера, чтобы получить требования к системе.	Прочтите требования к операционной системе в техническом замечании 1243309. Кроме того, смотрите рекомендации в документе Задачи по настройке для операционной системы и других приложений. Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Дополнительную информацию о том, как подобрать размер для сервера и хранения, смотрите в документе IBM Spectrum Protect Blueprint.
Сконфигурированы ли диски для оптимальной производительности?	Объем настройки, которую нужно производить для разных дисковых систем, различается. Убедитесь, что задана соответствующая глубина очереди и другие опции дисковых систем.	Дополнительные сведения смотрите в следующих разделах: • "Планирование для дисков базы данных сервера" • "Планирование для дисков журнала восстановления сервера" • "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли памяти на сервере?	Для более высоких рабочих нагрузок и таких дополнительных функций, как дедупликация данных и репликация узлов, требуется объем системной памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Для баз данных, не включенных для дедупликации данных, используйте следующие рекомендации по определению требований к системной памяти: • Для баз данных, объемом менее 500 ГБ, требуется 16 ГБ памяти. • Для баз данных, объемом от 500 ГБ до 1 ТБ, требуется 24 ГБ памяти. • Для баз данных, объемом от 1 ТБ до 1,5 ТБ, требуется 32 ГБ памяти. • Для баз данных, объем которых превышает 1,5 ТБ, требуется 40 ГБ памяти. Убедитесь, что вы выделили дополнительное пространство для активного и архивного журналов для обработки репликации.	Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов • Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Есть ли в системе достаточное число адаптеров шины хоста (host bus adapter, HBA) для обработки операций с данными, которые сервер IBM Spectrum Protect должен выполнять одновременно?	Определите, для каких операций требуется использовать HBA одновременно. Например, серверу нужно сохранять 1 ГБ/сек данных резервных копий и при этом также нужно производить перенастройку пула хранения, для выполнения чего требуется 0,5 ГБ/сек. HBA должны быть способны обрабатывать все эти данные с нужной скоростью.	Смотрите раздел Настройка емкости HBA.
Превышает ли ширина полосы пропускания сети запланированную максимальную пропускную способность для резервнных копий?	Полоса пропускания сети должна позволять системе выполнять такие операции, как резервное копирование, когда это разрешено или соответствует обязательствам на уровне услуг. Для репликации узлов полоса пропускания сети должна быть больше запланированной максимальной пропускной способности.	Дополнительные сведения смотрите в следующих разделах: • Настройка производительности сети • Контрольный список по репликации узлов
Используете ли вы предпочтительную файловую систему для файлов сервера IBM Spectrum Protect?	Используйте файловую систему, обеспечивающую оптимальную производительность и доступность данных. Сервер использует прямой ввод-вывод для файловых систем, поддерживающих эту функцию. Использование прямого ввода-вывода может повысить пропускную способность и уменьшить степень использования процессора. Более подробную информацию о предпочтительной файловой системе для вашей операционной системы смотрите в документе Файловые системы, поддерживаемые сервером IBM Spectrum Protect.	Дополнительную информацию смотрите в разделе Конфигурирование операционной системы для производительности дисков.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы сконфигурировать достаточное пространство подкачки?	Пространство подкачки (или свопинга) расширяет память, доступную для обработки. Если объем свободной RAM в системе мал, программы или данные, которые не используются, перемещаются из памяти в пространство подкачки. Это действие высвобождает память для других операций, например, операций базы данных.  Операционные системы Linux Используйте, как минимум, 32 ГБ пространства подкачки или 50% оперативной памяти в зависимости от того, какое значение будет больше.	
 Операционные системы Linux Собираетесь ли вы настроить параметры ядра после установки сервера?	 Операционные системы Linux Вы должны настроить параметры ядра.	 Операционные системы LinuxИнформацию о настройке параметров ядра смотрите в следующем документе: Linux: Настройка параметров ядра для систем Linux

Linux: Планирование для дисков базы данных сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Находится ли база данных на быстрых дисках с низкой латентностью?	Не используйте для базы данных IBM Spectrum Protect следующие накопители: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Не используйте внутренние диска, включенные по умолчанию в большинство аппаратных компонентов серверов. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность. Если вы собираетесь использовать функции дедупликации данных в IBM Spectrum Protect, обратите внимание на производительность дисков в виде числа операций ввода-вывода в секунду (I/O operations per second, IOPS).	Дополнительную информацию смотрите в разделе Контрольный список для дедупликации данных.
Хранится ли база данных на дисках или LUN отдельно от дисков или LUN, используемых для активного журнала, архивного журнала и томов пула хранения?	Если отделить базу данных сервера от других серверных компонентов, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно. Совет: База данных и архивный журнал могут совместно использовать массив, когда вы применяете технологию твердотельных накопителей (solid-state drive, SSD).	
Если вы используете RAID, знаете ли вы, как выбрать оптимальный уровень RAID для вашей системы? Задаете ли вы все LUN одного и того же размера и типа RAID?	Если системе нужно производить большое число операций записи, RAID 10 превосходит RAID 5. Однако для RAID 10 требуется больше дисков, чем для RAID 5 при одном и том же объеме используемого пространства хранения. Если в вашей дисковой системе используется RAID, задайте все ваши LUN с использованием одного и того же размера и типа RAID. Например, не смешивайте 4+1 RAID 5 с 4+2 RAID 6.	
Если доступна опция задать размер полосы или размер сегмента, планируете ли вы оптимизировать размер при конфигурировании дисковой системы?	Если вы можете задать размер полосы или размер сегмента, используйте в дисковых системах для базы данных размер, равный 64 КБ или 128 КБ.	Размер блока, используемого для базы данных, зависит от табличного пространства. Большинство таблиц используют блоки по 8 КБ, но некоторые используют блоки по 32 КБ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы создать хотя бы четыре каталога, которые также называются путями хранения, на четырех отдельных LUN для базы данных? Создайте по одному каталогу на отдельный массив в подсистеме. Если у вас менее трех массивов, создайте внутри массива отдельный том LUN.	При более высоких рабочих нагрузках и использовании некоторых функций требуется больше путей хранения, чем это соответствует минимальным требованиям. Такие операции сервера, как дедупликация данных, приводят к более высокому числу операций ввода-вывода в секунду (input/output operations per second, IOPS) для базы данных. Такие операции лучше выполняются, если у базы данных больше каталогов. В случае баз данных серверов, размер которых превышает 2 ТБ или которые, как ожидается, вырастут до этого размера, используйте восемь каталогов. При определении того, сколько путей хранения следует создать, рассмотрите запланированный рост системы. Сервер эффективнее использует высокое число путей хранения, если пути хранения присутствовали при первом создании сервера. Используйте переменную *DB2_PARALLEL_IO*, чтобы принудительно производить параллельный ввод-вывод в табличных пространствах, у которых один контейнер, или в табличных пространствах, контейнеры которых находятся более чем на одном физическом диске. Если вы не зададите переменную *DB2_PARALLEL_IO*, параллелизм ввода-вывода будет равен числу контейнеров, используемых табличным пространством. Например, если табличное пространство охватывает четыре контейнера, используемый уровень параллелизма ввода-вывода будет равен 4.	Дополнительные сведения смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Справку относительно того, как предсказать рост, когда сервер производит дедупликацию данных, смотрите в техническом замечании 1596944. Последнюю информацию о размере базы данных, реорганизации базы данных и замечания относительно производительности для серверов IBM Spectrum Protect смотрите в техническом замечании 1683633. Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Является ли размер всех каталогов для базы данных одинаковым?	Каталоги одного и того же размера обеспечивают одинаковую степень параллелизма для операций базы данных. Если размер одного или нескольких каталогов для базы данных меньше размера остальных каталогов, то потенциал оптимизированного предварительного извлечения снизится. Эта рекомендация также применима, если вам нужно добавить пути хранения после первоначального конфигурирования сервера.	
Собираетесь ли вы увеличить глубину очереди для LUN базы данных в системах AIX?	Глубина очереди по умолчанию часто оказывается слишком мала.	Смотрите раздел Конфигурирование систем AIX для производительности диска.

Linux: Планирование для дисков журнала восстановления сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Хранятся ли активный журнал и архивный журнал на дисках или на LUN отдельно от дисков или LUN, используемых для базы данных и томов пула хранения?	Убедитесь, что диски, на которых вы размещаете активный журнал, не используются для других задач сервера или системы. Не помещайте активный журнал на диски, содержащие базу данных сервера, архивный журнал или такие системные файлы, как пространство подкачки или свопинга.	Если отделить базу данных сервера, активный журнал и архивный журнал, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно.
Находятся ли журналы на дисках с энергонезависимым кэшем записи?	Энергонезависимый кэш записи позволяет как можно быстрее записывать данные в журналы. Более быстрые операции записи для журналов могут повысить производительность операций сервера.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задаете ли вы для журналов размер, который адекватно поддерживает рабочую нагрузку?	Если вы не уверены относительно рабочей нагрузки, используйте самый большой возможный для вас размер. Активный журнал Максимальный размер - 512 ГБ, заданный с помощью опции сервера ACTIVELOGSIZE. Убедитесь, что у вас есть хотя бы 8 ГБ свободного пространства в файловой системе активного журнала после создания активных журналов фиксированного размера. Архивный журнал Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что размер архивного журнала, как минимум, равен размеру активного журнала.	• Подробную информацию о размерах журналов смотрите в информации о журнале восстановления в техническом замечании 1421060. • Информацию о подборе размеров при использовании дедупликации данных смотрите в разделе Контрольный список для дедупликации данных.
Задаете ли вы архивный журнал передачи управления при отказе? Размещаете ли вы этот журнал на диске, являющемся отдельным по сравнению с диском архивного журнала?	Архивный журнал передачи управления при отказе предназначен для использования сервером в аварийных ситуациях, когда архивный журнал переполняется. Для архивного журнала передачи управления при отказе можно использовать более медленные диски.	Используйте опцию сервера ARCHFAILOVERLOGDIRECTORY, чтобы указать расположение архивного журнала передачи управления при отказе. Отслеживайте использование каталога для архивного журнала передачи управления при отказе. Если архивный журнал передачи управления при отказе должен использоваться сервером, пространство архивного журнала может оказаться недостаточным.
Если вы производите зеркальное отображение активного журнала, используете ли вы только один тип зеркального отображения?	Зеркальное отображение журнала можно производить, используя один из описанных ниже методов. Используйте для журнала только один тип зеркального отображения. • Используйте опцию MIRRORLOGDIRECTORY, которая доступна для сервера IBM Spectrum Protect, чтобы задать расположение зеркального отображения. • Используйте в AIX зеркальное отображение программ, например, Logical Volume Manager (LVM). • Используйте зеркальное отображение на оборудовании дисковых систем.	Если вы зеркально отображаете активный журнал, убедитесь, что у дисков для активного журнала и зеркальной копии одинаковая скорость и надежность. Дополнительную информацию смотрите в разделе Конфигурирование и настройка журнала восстановления.

Linux: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров

Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы быстрое дисковое хранения для базы данных IBM Spectrum Protect, если измерять ее в операциях ввода-вывода в секунду (input/output operations per second, IOPS)?	Используйте для базы данных высокопроизводительный диск. Используйте технологию твердотельных дисков для обработки дедупликации данных. Убедитесь, что база данных обеспечивает минимальное значение в 3000 IOPS. Для каждого терабайта данных, копируемого в день (до дедупликации данных) прибавьте к этому минимуму 1000 IOPS. Например, для сервера IBM Spectrum Protect, который пропускает 3 ТБ данных в день, потребуется 6000 IOPS для дисков базы данных: `минимум 3000 IOPS + 3000 (3 ТБ x 1000 IOPS) = 6000 IOPS`	Рекомендации относительно выбора диска смотрите в разделе "Планирование для дисков базы данных сервера". Дополнительные сведения об IOPS смотрите в документах IBM Spectrum Protect Макеты.
Достаточно ли памяти для размера вашей базы данных?	Для серверов IBM Spectrum Protect с размером базы данных, равным 100 ГБ, которые производят дедупликацию данных, используйте, как минимум, 40 ГБ системной памяти. Если сохраняемый объем данных резервных копий возрастает, может понадобиться увеличить требования к системной памяти. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память. Используйте больше памяти, чтобы улучшить кэширование страниц базы данных. Приведенные ниже рекомендация по размеру памяти основаны на ежедневном объеме новых данных, резервные копии которых вы создаете: • 128 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 1-2 ТБ • 192 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 2-4 ТБ	Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Правильно ли вы подобрали размер емкости хранения для активного и архивного журналов базы данных?	Сконфигурируйте для сервера минимальный размер активного журнала 128 Гбайт, задав для опции сервера ACTIVELOGSIZE значение 131072. Рекомендуемый начальный размер архивного журнала - 1 ТБ. Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что для файловой системы есть хотя бы 10% дополнительного пространства на диске, превышающего размер архивного журнала. Используйте для архивных журналов баз данных каталог с начальной свободной емкостью, как минимум, 1 ТБ. Задайте каталог при помощи опции сервера ARCHLOGDIRECTORY. Определите пространство для архивного журнала восстановления после отказа при помощи опции сервера ARCHFAILOVERLOGDIRECTORY.	Дополнительную информацию о том, как подобрать размер системы, смотрите в документах IBM Spectrum Protect Макеты.
Включено ли сжатие для архивного журнала и резервных копий базы данных?	Включите опцию сервера ARCHLOGCOMPRESS, чтобы сэкономить пространство хранения. Эта опция сжатия отличается от строенного сжатия. Встроенное сжатие по умолчанию включено в IBM Spectrum Protect V7.1.5 и новее. Ограничение: Не используйте эту опцию, если объем резервных копий данных превышает 6 ТБ в день.	Дополнительную информацию о сжатии для вашей системы смотрите в документах IBM Spectrum Protect Макеты.
Расположены ли база данных и журналы IBM Spectrum Protect в разных томах диска (LUN)? Сконфигурирован ли диск, который используется для базы данных, в соответствии с рекомендациями для транзакционной базы данных?	База данных не должна использовать дисковые тома совместно с журналами или пулами хранения IBM Spectrum Protect, с другим приложением или с другой файловой системой.	Дополнительную информацию о базе данных сервера и конфигурации журнала восстановления смотрите в документе Конфигурирование и настройка базы данных сервера и журнала восстановления.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы, как минимум, восемь (2,2 ГГц или эквивалент) ядер процессора для каждого сервера IBM Spectrum Protect, который вы хотите использовать в сочетании с дедупликацией данных?	Если планируется использование дедупликации данных на стороне клиента, проверьте, есть ли у систем клиентов адекватные ресурсы, доступные во время операции резервного копирования, чтобы выполнять обработку дедупликации данных. Используйте процессор, эквивалентный по крайней мере одному процессорному ядру 2,2 ГГц, на каждый процесс резервного копирования с дедупликацией данных на стороне клиента.	• Эффективное планирование и использование дедупликации • IBM Spectrum Protect Макеты
Выделен ли вами достаточный объем пространства хранения для базы данных?	В первом приближении нужно запланировать выделение 100 ГБ для хранения базы данных на каждые 50 ТБ данных, которые будут защищены в дедуплицированных пулах хранения. *Защищенные данные* - это объем данных перед дедупликацией данных, включая все версии сохраненных объектов. Лучше всего задать новый пул хранения исключительно для дедупликации данных. Дедупликация данных производится на уровне пула хранения. Дедупликации подвергаются все данные, содержащиеся в пуле хранения, за исключением зашифрованных данных.	
Оценили ли вы емкость пула хранения для конфигурирования достаточного пространства, соответствующего размеру вашей среды?	Для оценки требований к емкости для дедуплицированного пула хранения можно использовать следующий метод: 1. Оцените базовый размер данных источника. 2. Оцените ежедневный размер резервных копий, используя предполагаемый темп изменений и роста. 3. Определите требования к сроку хранения. 4. Вычислите общий размер данных данных источника с учетом базового размера, ежедневного размера резервных копий и требований к сроку хранения. 5. Примените коэффициент дедупликации. 6. Примените коэффициент сжатия. 7. Округлите оценку, чтобы учесть переходное использование пула хранения.	Пример использования этого метода смотрите на веб-странице Эффективное планирование и использование дедупликации.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Распределили ли вы операции дискового ввода-вывода по нескольким дисковым устройствам и контроллерам?	Используйте массивы, которые состоят из как можно большего количества дисков (иногда это называется 'широкое чередование'. Убедитесь, что вы используете один каталог базы данных для отдельного массива в подсистеме. Задайте переменную реестра *DB2_PARALLEL_IO*, так чтобы включить параллельный ввод-вывод для каждого табличного пространства, используемого, если контейнеры в табличном пространстве охватывают несколько физических дисков. Если полоса пропускания для ввода-вывода доступна, а размер файлов велик (например, 1 МБ), процесс нахождения дубликатов может использовать ресурсы всего процессора. Когда файлы меньше, более критичны другие узкие места. Задайте восемь или больше файловых систем для класса устройств дедуплицированного пула хранения, чтобы операции ввода-вывода распределялись по максимально возможному числу LUN и физических устройств.	Рекомендации по настройке пулов хранения смотрите в разделе "Планирование для пулов хранения на устройствах классов устройств DISK или FILE". Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.
Запланировали ли вы ежедневные операции на основе вашей стратегии резервного копирования?	Наилучшая последовательность операций будет следующей: 1. Резервное копирование клиента 2. Защита пула хранения 3. Репликация узлов 4. Резервное копирование базы данных 5. Окончание действия устаревших файлов	• Планирование дедупликации данных и процессов репликации узла • Ежедневные операции для пулов хранения каталогов-контейнеров

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли у вас пространства хранения для управления списком блокировки DB2?	Если выполняется дедупликация данных, в состав которых входят большие объекты или большое число одновременно обрабатываемых файлов, процесс может привести к тому, что станет не хватать пространства хранения. При нехватке пространства хранения списка блокировок могут происходить ошибки резервного копирования, отказы процессов управления данными или перерывы в работе сервера. Если дедупликация данных обрабатывает файлы размером более 500 ГБ, это вероятнее всего приведет к истощению пространства хранения. Но если большое число выполняемых операций резервного копирования использует дедупликацию данных на стороне клиента, эта проблема может также произойти и с файлами меньшего размера.	Информацию о настройке параметра DB2 LOCKLIST смотрите в документе Настройка дедупликации данных на стороне сервера.
Доступна ли достаточная полоса пропускания для передачи данных на сервер IBM Spectrum Protect?	Чтобы переносить данные на сервер IBM Spectrum Protect, используйте дедупликацию данных на стороне клиента или на стороне сервера и сжатие, чтобы уменьшить необходимую ширину полосы пропускания. Используйте сервер V7.1.5 или новее, чтобы применить встроенное сжатие, и используйте клиент V7.1.6 или новее, чтобы включить усовершенствованную обработку сжатия.	Дополнительные сведения смотрите в описании опции клиента enablededup.
Определили ли вы, сколько каталогов пула хранения следует назначить для каждого пула хранения?	Назначьте каталоги для пула хранения, используя команду DEFINE STGPOOLDIRECTORY. Создайте несколько каталогов пула хранения и убедитесь, что для каждого каталога создается резервная копия на отдельном дисковом томе (LUN).	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Выделен ли вами достаточный объем дискового пространства в пуле хранения облачных контейнеров?	Чтобы предотвратить ошибки резервного копирования, убедитесь, что в локальном каталоге достаточно места. Оптимальный размер дискового пространства указан ниже в списке: • Для SCSI с последовательным подключением (SAS) и вращающегося диска вычислите объем новых данных, ожидаемых поле ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства. • Для систем хранения на основе флэш-памяти, у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 3 Тбайт. • Для систем хранения с твердотельными накопителями (SSD), у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 5 Тбайт.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Выбрали ли вы подходящий тип локальной системы хранения?	Убедитесь, что передача данных из локальной системы хранения в облако завершена до начала следующего цикла резервного копирования.
	Совет: Данные удаляются из локальной системы хранения вскоре после их перемещения в облако.
	Учтите следующие рекомендации:
	• Используйте флеш-память или твердотельные накопители (SSD) для больших облачных система высокой производительности. Убедитесь, что у вас есть ссылка на глобальную сеть (wide area network, WAN) с выделенными 10 Гбайт памяти и высокоскоростным соединением с хранилищем объектов. Например, используйте флеш-память или SSD, если у вас выделенная ссылка 10 ГБ WAN плюс высокоскоростное соединение либо с расположением IBM® Cloud Object Storage, либо с центром данных Amazon Simple Storage Service (Amazon S3).
	• Для указанных ниже сценариев используйте диски SAS большей емкости 15000 rpm:
	  ○ Системы среднего размера
	  ○ Медленные соединения с облаком, например 1 Гбайт
	  ○ При использовании IBM Cloud Object Storage в качестве провайдера службы в нескольких регионах
	• Для SAS или вращающегося диска вычислите объем новых данных, ожидаемых после ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства.	

Linux: Планирование для пулов хранения на устройствах классов устройств DISK или FILE

Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Могут ли LUN пула хранения поддерживать пропускную способность для последовательного чтения и записи, объемом 256 КБ, чтобы адекватно обрабатывать рабочую нагрузку в пределах ограничений времени?	При планировании пиковых нагрузок учитывайте все данные, которые сервер должен читать из дисковых пулов хранения или записывать в дисковые пулы хранения одновременно. Например, рассмотрим пиковый поток данных от одновременно выполняющихся операций резервного копирования клиента и операций по перемещению данных сервером, например, перенастройку. В подавляющем большинстве случаев сервер IBM Spectrum Protect производит чтение из пулов хранения и записывает данные в пулы хранения блоками по 156 КБ. Если дисковая система обеспечивает такую возможность, сконфигурируйте дисковую систему для оптимальной производительности при выполнении последовательных операций чтения/записи, а не случайных операций чтения/записи.	Дополнительную информацию смотрите в документе Анализ базовой производительности дисковых систем.
Сконфигурирован ли диск для использования кэша чтения и записи?	Используйте больший объем кэша, чтобы повысить производительность.	
Определили ли вы правильный размер, который следует использовать для томов пула хранения, когда пулы хранения используют класс устройств FILE?	Ознакомьтесь с информацией в разделе Оптимальное число и размер томов для пулов хранения, использующих диск. Если у вас нет информации, которая бы позволила оценить размер томов класса устройств FILE, начните с томов, имеющих 50 ГБ.	Как правило, проблемы чаще возникают, если тома слишком малы. Если тома больше, чем требуется, сообщается о малом числе проблем. Когда вы определите размер тома, который следует использовать, в качестве предосторожности выберите размер, который может оказаться больше необходимого.
Используете ли вы заранее выделенные тома для пулов хранения, использующих классы устройств FILE?	Чистые тома могут вызвать фрагментацию файлов. Чтобы убедиться, что пулу хранения будет хватать томов, задайте для параметра MAXSCRATCH значение больше нуля.	Используйте серверную команду DEFINE VOLUME, чтобы заранее выделить тома в пуле хранения. Используйте серверную команду DEFINE STGPOOL или UPDATE STGPOOL, чтобы задать параметр MAXSCRATCH.
Сравнивали ли вы максимальное число сеансов клиентов с числом заданных томов для пулов хранения, использующих классы устройств FILE?	Всегда оставляйте в пулах хранения достаточное число пригодных для использования томов, чтобы разрешить одновременное выполнение ожидаемого пикового числа сеансов клиентов. Тома могут быть чистыми, пустыми или частично заполненными томами.	В случае пулов хранения, которые используют класс устройств FILE, на том одновременно может производить запись только один сеанс или процесс.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задали ли вы для параметра MOUNTLIMIT класса устройств достаточно высокое значение, чтобы учесть число томов, которые могут быть смонтированы параллельно, когда пулы хранения используют класс устройств FILE?	Для пулов хранения, использующих дедупликацию данных, параметр MOUNTLIMIT, как правило, находится в диапазоне 500-1000. Задайте для MOUNTLIMIT значение, равное максимальному числу необходимых точек монтирования, необходимых для всех активных сеансов. Рассмотрим параметры, которые влияют на максимальное число необходимых точек монтирования: • Опция сервера MAXSESSIONS, представляющая собой максимальное число сеансов IBM Spectrum Protect, которые могут выполняться одновременно. • Параметр MAXNUMMP, указывающий, какое максимальное число точек монтирования может использовать каждый клиентский узел. Например, если максимальное число сеансов резервного копирования клиентских узлов, как правило, составляет 100, а для каждого из узлов задан параметр `MAXNUMMP=2`, умножьте 100 узлов на 2 точки монтирования для каждого узла, чтобы получить значение 200 для параметра MOUNTLIMIT.	Используя серверную команду REGISTER NODE или UPDATE NODE, задайте параметр MAXNUMMP для клиентских узлов.
Определили ли вы, сколько томов пула хранения поместить в каждую файловую систему для пулов хранения, использующих классы устройств DISK?	То, как вы конфигурируете пространство хранения для пула хранения, использующего класс устройств DISK, зависит от того, используете ли вы RAID для дисковой системы. Если вы не используете RAID, сконфигурируйте по одной файловой системе на физический диск и задайте по одному тому пула хранения для каждой файловой системы. Если вы используете RAID 5 с *n*+1 томами, сконфигурируйте пространство хранения одним из следующих способов: • Сконфигурируйте *n* файловых систем на LUN и задайте по одному тому пула хранения для файловой системы. • Сконфигурируйте одну файловую систему и *n* томов пула хранения для LUN.	Пример схемы, соответствующей этой рекомендации, смотрите в документе Пример схемы пулов хранения сервера.
Создали ли вы пулы хранения для распределения операций ввода-вывода по нескольким файловым системам?	Убедитесь, что каждая файловая система находится на отдельном LUN в дисковой системе. Как правило, 10-30 файловых систем - это оптимальная цель, но вы должны убедиться, что размер файловых систем будет не менее, чем 250 ГБ (примерно).	Дополнительные сведения смотрите в следующих разделах: • Настройка дискового хранения для сервера • Настройка и конфигурирование пулов хранения и томов

Linux: Планирование правильного типа технологии хранения

У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.

Процедура

Ознакомьтесь со следующей таблицей, которая поможет вам выбрать правильный тип технологии хранения для ресурсов хранения, необходимых серверу.

Табл. 1. Типы технологии хранения в требованиях по хранению IBM Spectrum Protect

Тип технологии хранения	**Database**	**Активный журнал**	**Архивный журнал и резервный архивный журнал**	**Пулы хранения**
Твердотельный диск (Solid-state disk, SSD)	Размещайте базу данных на SSD при следующих обстоятельствах: • Вы используете дедупликацию данных IBM Spectrum Protect. • Вы ежедневно производите резервное копирование более чем 8 ТБ новых данных.	Если вы поместите базу данных IBM Spectrum Protect на SSD, лучше всего поместить активный журнал на SSD. Если пространство недоступно, используйте вместо этого высокопроизводит. диск.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Архивный журнал и архивные журналы передачи управления при отказе можно поместить на носители с более медленными типами технологии хранения.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Пулы хранения можно поместить на носители с более медленными типами технологии хранения.
Высокопроизв. диск со следующими хар-ками: • **Диск 15 К rpm** • **Оптоволокно (Fibre Channel) интерфейс или последов. подкл. интерфейс SCSI (SAS).**	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Высокопроизв. диски можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте высокопроизв. диски для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.

Тип технологии хранения	Database	Активный журнал	Архивный журнал и резервный архивный журнал	Пулы хранения
Диск средней произв. или высокопроизв. диск со следующими хар-ками: • **Диск 10 K rpm** • **Оптоволокно (Fibre Channel) интерфейс или интерфейс SAS**	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Диск средней производительности или высокопроизв. диск можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте диск средней производительности или высокопроизв. диск для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.
SATA, пространство хранения, подключенное к сети	Не используйте этот тип хранения для базы данных. Не помещайте базу данных в системы хранения XIV.	Не используйте этот тип хранения для активного журнала.	Использование этой более медленной технологии хранения является приемлемым, так как эти журналы записываются один раз и редко читаются.	Используйте эту более медленную технологию хранения при следующих обстоятельствах: • Данные редко записываются, например, записываются один раз. • Данные редко читаются. .
Лента и виртуальная лента				Используйте для долгосрочного хранения, если данные используются нечасто.

Linux: Применение наилучших практических методов к установке сервера

Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Процедура

- Описанные ниже наилучшие методы являются наиболее важными для достижения оптимальной производительности и предотвращения ошибок.
- Смотрите таблицу, чтобы определить наилучшие методы, применимые к вашей среде.

Практическая рекомендация	Дополнительная информация
Используйте для базы данных сервера быстрые диски. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность.	Используйте для базы данных быстрые диски с низкой латентностью. Использование SSD является существенным, если вы используете дедупликацию данных и репликацию узлов. Старайтесь не использовать диски Serial Advanced Technology Attachment (SATA) и Parallel Advanced Technology Attachment (PATA). Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование правильного типа технологии хранения"
Убедитесь, что в системе сервера достаточно памяти.	Прочтите требования к операционной системе в техническом замечании 1243309. При более высоких рабочих нагрузках требуется больше ресурсов, чем указано в минимальных требованиях. Такие дополнительные функции, как дедупликация данных и репликация узлов, могут потребовать объем памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Если вы планируете запускать несколько экземпляров сервера, каждому экземпляру потребуется объем памяти, указанный для одного сервера. Умножьте объем памяти для одного сервера на число экземпляров, которые вы собираетесь запускать в системе.
Отделите базу данных сервера, активный журнал, архивный журнал и дисковые пулы хранения друг от друга.	Держите все ресурсы хранения IBM Spectrum Protect на отдельных дисках. Держите диски пулов хранения храниться отдельно от дисков базы данных сервера и журналов. Операции пулов хранения могут перекрываться операциями базы данных, если они находятся на одних и тех же дисках. В идеале база данных сервера и журналы также должны быть отделены друг от друга. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование для дисков журнала восстановления сервера" ○ "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"
Используйте для базы данных сервера хотя бы четыре каталога. Для больших серверов или серверов, использующих дополнительные функции, используйте восемь каталогов.	Поместите каждый каталог на LUN, изолированный от других LUN и от других приложений. Сервер считается большим, если его база данных превышает 2 ТБ или если ожидается, что она вырастет больше этого размера. Используйте для таких серверов восемь каталогов. Смотрите раздел "Планирование для дисков базы данных сервера".
Если вы используете дедупликацию данных и/или репликацию узлов, следуйте рекомендациям по конфигурированию базы данных и других элементов.	Сконфигурируйте базу данных сервера в соответствии с рекомендациями, так как база данных чрезвычайно важна для того, чтобы сервер смог хорошо работать, если используются такие функции. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ Контрольный список для дедупликации данных ○ Контрольный список по репликации узлов

Практическая рекомендация	Дополнительная информация
В случае пулов хранения, которые используют класс устройств типа FILE, выполните рекомендации по размеру томов пула хранения. Как правило, тома 50 ГБ подходят лучше всего.	Прочтите информацию в разделе Оптимальное число и размер томов для пулов хранения, использующих диск, чтобы это помогло вам определить размер тома. Сконфигурируйте устройства пула хранения и файловые системы на основе требований к пропускной способности, а не только на основе требований к емкости. Изолируйте устройства хранения, используемые продуктом IBM Spectrum Protect, от других приложений с высоким объемом ввода-вывода и убедитесь, что для этого хранилища обеспечивается достаточная пропускная способность. Дополнительные сведения смотрите в разделе Контрольный список для пулов хранения на устройствах DISK или FILE.
Запланируйте операции клиента IBM Spectrum Protect и действия по обслуживанию сервера, чтобы избежать перекрывания операций или свести такое перекрывание к минимуму.	Дополнительные сведения смотрите в следующих разделах: ◦ Настройка расписания для ежедневных операций ◦ Контрольный список для конфигурации сервера
Постоянно осуществляйте мониторинг операций.	Проводя мониторинг, вы сможете раньше находить ошибки и вам будет проще выявлять их причины. Срок хранения записей отчетов мониторинга может доходить до года - это поможет вам выявлять тенденции и планировать рост. Смотрите раздел Мониторинг среды и ее обслуживание с целью обеспечения производительности.

Linux: Минимальные требования к системе для систем Linux

Чтобы установить сервер IBM Spectrum Protect в системе Linux, требуется минимальный уровень аппаратного и программного обеспечения, включая способ связи и самую последнюю версию драйверов устройств.

Оптимальная среда IBM Spectrum Protect настраивается с дедупликацией данных с использованием IBM Spectrum Protect Blueprints.

Пакет драйверов устройств IBM Spectrum Protectне содержит драйвер устройств для этой операционной системы, так как используется типовой драйвер устройств SCSI. Сконфигурируйте драйвер устройств до использования сервера IBM Spectrum Protect с ленточными устройствами. Пакет драйверов IBM Spectrum Protect содержит инструменты драйверов и демоны ACSLS. Найти драйверы устройств IBM® можно на сайте Fix Central.

Требования, информация о поддерживаемых устройствах, пакеты установки клиента и исправления можно получить по адресу: IBM для IBM Spectrum Protect. После установки IBM Spectrum Protect и до настройки этого продукта посетите этот веб-сайт и скачайте и примените все применимые исправления.

-  Операционные системы LinuxLinux: Минимальные требования к серверу Linux x86_64
  Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux x86_64, ознакомьтесь с требованиями к аппаратному и программному обеспечению.
-  Операционные системы LinuxLinux: Минимальные требования к серверу Linux on System z
  Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on System z, ознакомьтесь с требованиями к аппаратному и программному обеспечению.
-  Операционные системы LinuxLinux: Минимальные требования к серверу Linux on Power Systems (с прямым порядком байтов)
  Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on Power Systems (с прямым порядком байтов), ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Linux: Минимальные требования к серверу Linux x86_64

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux x86_64, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

Linux: Минимальные требования к серверу Linux on System z

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on System z, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

Linux: Минимальные требования к серверу Linux on Power Systems (с прямым порядком байтов)

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Linux on Power Systems (с прямым порядком байтов), ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

Операционные системы Linux

Linux: Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе

При определенных ограничениях на одном компьютере с сервером IBM Spectrum Protect версии 8.1.5 можно установить другие продукты, которые тоже внедряют и используют DB2.

Если вы хотите установить и использовать другие продукты, которые используют продукт DB2, на одном компьютере с сервером IBM Spectrum Protect, убедитесь, что выполняются следующие условия:

Табл. 1. Совместимость сервера IBM Spectrum Protect с другими продуктами DB2 в системе

Критерий	**Инструкции**
Уровень версии	Другие продукты, использующие DB2, должны использовать DB2 версии 9 или новее. Продукты DB2 включают в себя поддержку инкапсуляции и разделения продуктов, начиная с версии 9. Начиная с этой версии, можно запускать несколько копий продуктов DB2 с разными уровнями кода в одной системе. Чтобы узнать об этом подробнее, смотрите информацию о нескольких копиях DB2 по адресу: Информация о DB2.

Критерий	Инструкции
ID и каталоги пользователей	Убедитесь, что ID пользователей, ID изолированных пользователей, положение установки, другие каталоги и связанная информация не используются одновременно в нескольких установках DB2. Ваши спецификации должны отличаться от тех ID и положений, которые использовались для установки и конфигурирования сервера IBM Spectrum Protect. Если вы сконфигурировали сервер при помощи мастера dsmicfgx, это будут значения, введенные вами во время работы с мастером. Если вы использовали метод конфигурирования вручную, вспомните, какие значения вы использовали для сервера при выполнении этих процедур (если это потребуется).
Выделение ресурсов	Оцените ресурсы и возможности системы, сопоставив их как с требованиями для сервера IBM Spectrum Protect, так и для других программ, которые используют продукт DB2. Чтобы обеспечить достаточно ресурсов для других приложений DB2, нужно изменить параметры сервера IBM Spectrum Protect, так чтобы сервер использовал меньше памяти и ресурсов. Аналогичным образом, если рабочие нагрузки для других приложений DB2 таковы, что между этими приложениями и сервером IBM Spectrum Protect возникает конфликт доступа к ресурсам процессора или памяти, это может отрицательно сказаться на производительности сервера при обработке ожидаемой рабочей нагрузке клиента или при выполнении других серверных операций. Чтобы разделить ресурсы и обеспечить больше возможностей настройки и распределения ресурсов процессора и памяти и других системных ресурсов между несколькими приложениями, рассмотрите возможность использования логических разделов (Logical Partition - LPAR), разделов рабочей нагрузки (Workload Partition - WPAR) или иной поддержки виртуальных рабочих станций. Например, запускайте программу DB2 в ее собственной виртуальной системе.

Linux: IBM Installation Manager

IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке IBM Spectrum Protect. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать IBM Spectrum Protect.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение
: Устанавливаемый модуль программного продукта.

  Предложение IBM Spectrum Protect содержит все носители, которые требуются IBM Installation Manager для установки IBM Spectrum Protect.

Пакет
: Группа программных компонентов, необходимых для установки предложения.
  Пакет IBM Spectrum Protect включает в себя следующие компоненты:

  - Программа установки IBM Installation Manager
  - Предложение IBM Spectrum Protect

Группа пакетов
: Набор пакетов, использующих общий родительский каталог.

  Группа пакетов по умолчанию для пакета IBM Spectrum Protect - `IBM Installation Manager`.

Репозиторий
: Удаленная или локальная область хранения данных и других ресурсов программы.

Пакет IBM Spectrum Protect хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
: Каталог, содержащий файлы или подключаемые модули программ, которые совместно используются пакетами.

  IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии IBM Spectrum Protect.

Linux: Контрольные списки для планирования сведений о сервере

Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.

Элемент	Необходимое пространство	Число каталогов	Положение каталогов
База данных			
Активный журнал			
Архивный журнал			
Необязательно: Зеркальная копия активного журнала			
Необязательно: Вторичный архивный журнал (резервный каталог для архивного журнала)			

Элемент	Имена и ID пользователей	Расположение
ID пользователя экземпляра для сервера, то есть ID, который использовался для запуска и работы сервера IBM Spectrum Protect		
Домашний каталог для сервера, то есть каталог, содержащий ID пользователя экземпляра		
Имя экземпляра базы данных		
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)		
Имя сервера; для каждого сервера используйте уникальное имя		

Linux: Планирование мощностей

Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.

- Linux: Оценка необходимого объема пространства для базы данных
  Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.

- Linux: Требования к пространству журнала восстановления
  В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.
- Linux: Мониторинг использования пространства для базы данных и журналов восстановления
  Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.
- Linux: Удаление файлов отката установки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Linux: Оценка необходимого объема пространства для базы данных

Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.

Об этой задаче

В качестве начального объема пространства базы данных можно порекомендовать использовать не менее 25 ГБ. Доступ к пространству файловой системы предоставляется должным образом. Размер базы данных 25 ГБ достаточен для среды тестирования или среды, включающей только менеджер библиотек. Для производственного сервера с поддержкой клиентских рабочих нагрузок размер базы данных должен быть больше. Если вы используете дисковые пулы хранения с произвольным доступом (DISK), потребуется дополнительное пространство хранения баз данных и журналов для пулов хранения с последовательным доступом.

Максимальный размер базы данных IBM Spectrum Protect - 6 ТБ.

Информацию об оценке размера базы данных в производственной среде на основе числа файлов и размера пула хранения смотрите в темах ниже.

- Linux: Оценка требований к пространству базы данных на основе числа файлов
  Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.
- Linux: Оценка требований к пространству базы данных на основе мощности пула хранения
  Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.
- Linux: Менеджер баз данных и временное пространство
  Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Linux: Оценка требований к пространству базы данных на основе числа файлов

Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.

Об этой задаче

Для оценки требований к объему пространства на основе максимального числа файлов в системе хранения сервера используйте следующие рекомендации:

- 600 - 1000 байт на каждую хранимую версию файла, включая резервные копии образов.
  Ограничение: Сюда не входит пространство, используемое во время дедупликации данных.

- 100 - 200 байт на каждый кэшированный файл, файл пула хранения копий, файл пула активных данных и дедуплицированный файл.
- Дополнительное пространство требуется для оптимизации базы данных в части поддержки переменных схем доступа к данным и внутренней обработки данных на сервере. Объем дополнительного пространства равен 50% оцененного размера памяти для хранения файловых объектов.

В следующем примере для единственного клиента вычисления основываются на максимальных значениях из предыдущих инструкций. В примерах не учитывается возможное использование объединения файлов. В общем случае объединение файлов сокращает объем требуемого пространства базы данных. Объединение файлов не затрагивает перенесенные файлы.

Процедура

1. Вычислите число версий файлов. Чтобы получить число версий файлов, сложите следующие значения:
   a. Вычислите число резервных копий файлов. Например, одновременно может существовать до 500 000 резервных копий клиентских файлов. В этом примере политики хранения требуют, чтобы хранилось до трех резервных копий каждого файла:

      ```
      500 000 файлов * 3 копии = 1 500 000 файлов
      ```

   b. Вычислите количество архивных файлов. Например, до 100 000 клиентских файлов могут быть архивными копиями.
   c. Вычислите количество перенесенных файлов. Например, до 200 000 клиентских файлов могут быть перемещены с клиентских рабочих станций.

   Если для каждого файла требуется 1000 байт, то общий объем требуемого для принадлежащих клиентам файлов пространства базы данных - 1,8 ГБ.

   ```
   (1 500 000 + 100 000 + 200 000) * 1000 = 1,8 ГБ
   ```

2. Вычислите число кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов:
   a. Вычислите количество кэшированных копий. Например, кэширование разрешено в дисковом пуле хранения размером 5 ГБ. Верхний порог переноса пула равен 90%, а нижний - 70%. Таким образом, 20% дискового пула, то есть 1 ГБ, будет занято кэшированными файлами.
      Если средний размер файла около 10 КБ, в кэше в любой момент времени находится около 100000 файлов:

      ```
      100 000 файлов * 200
      байт = 19 МБ
      ```

   b. Вычислите количество файлов пула хранения копий. Для всех основных пулов памяти создается резервная копия:

      ```
      (1 500 000 + 100 000 + 200 000) * 200 байт = 343 МБ
      ```

   c. Вычислите количество активных файлов пула хранения. Все данные активных резервных копий клиента в первичных пулах хранения копируются в пул хранения активных данных. Допустим, что 500 000 версий 1 500 000 резервных копий файлов в основном пуле являются активными:

      ```
      500 000 * 200 байт = 95 МБ
      ```

   d. Вычислите количество дедуплицированных данных. Допустим, что пул хранения данных, подвергнутых дедупликации, содержит 50000 файлов:

      ```
      50 000 * 200 байт = 10 МБ
      ```

   На основании этих вычислений для клиентских кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов требуется примерно 0,5 ГБ дополнительного пространства базы данных.
3. Вычислите объем дополнительного пространства, требуемый для оптимизации базы данных. Для обеспечения оптимального доступа к данным и управления сервером требуется дополнительное пространство базы данных. Объем дополнительного пространства базы данных равен 50% общего пространства, необходимого для хранения файловых объектов.

   ```
   (1,8 + 0,5) * 50% = 1,2 ГБ
   ```

4. Вычислите общий объем пространства базы данных, требуемый для этого клиента. Общий объем составит примерно 3,5 ГБ:

```
1,8 + 0,5 + 1,2 = 3,5 ГБ
```

5. Вычислите общий объем пространства базы данных, требуемый для всех клиентов. Если предыдущие оценки приведены для типичного клиента и у вас 500 таких клиентов, то можно использовать для примера следующую оценку общего объема пространства базы данных, требуемого для всех клиентов:

```
500 * 3,5 = 1,7 ТБ
```

Результаты

Совет: В приведенных выше примерах результаты представляют собой примерные оценки. Фактический размер базы данных может отличаться от ожидаемого из-за таких факторов, как число каталогов и длина полных имен файлов. Рекомендуется периодически производить мониторинг базы данных и корректировать ее размер, если потребуется.

Дальнейшие действия

При обычных операциях серверу IBM Spectrum Protect может потребоваться временное пространство баз данных. Это пространство необходимо для следующих задач:

- Сохранять результаты сортировки или упорядочивания, которые еще не сохранены и не оптимизированы непосредственно в базе данных. Эти результаты временно сохраняются в базе данных для обработки.
- Предоставлять административный доступ к базе данных одним из следующих способов:
  - Через клиент Open Database Connectivity (ODBC) DB2
  - Через клиент Oracle Java™ Database Connectivity (JDBC)
  - Из командной строки клиента администрирования на сервер с помощью Structured Query Language (SQL)

Используйте дополнительные 50 ГБ временного пространства на каждые 500 ГБ пространства для файловых объектов и оптимизации. Смотрите инструкции в следующей таблице. В примере, использованном в предыдущем шаге, для файловых объектов и оптимизации для 500 клиентов требуется общий объем пространства базы данных 1,7 ТБ. На основании этих оценок еще около 200 ГБ требуется для временного пространства. Суммарный объем требуемого пространства базы данных составляет 1,9 ТБ.

Размер базы данных	Минимальные потребности временного пространства
< 500 ГБ	50 ГБ
≥ 500 ГБ и < 1 ТБ	100 ГБ
≥ 1 ТБ и < 1,5 ТБ	150 ГБ
≥ 1,5 и < 2 ТБ	200 ГБ
≥ 2 и < 3 ТБ	250 - 300 ГБ
≥ 3 и < 4 ТБ	350 - 400 ГБ

Linux: Оценка требований к пространству базы данных на основе мощности пула хранения

Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.

Linux: Менеджер баз данных и временное пространство

Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Менеджер баз данных сортирует данные в определенном порядке, как в операторе SQL, который вводится для запроса данных. В зависимости от рабочей нагрузки на сервере, если объем данных больше, чем может обрабатывать менеджер баз данных, эти упорядоченные данные размещаются во временном дисковом пространстве. Данные располагаются во

временном дисковом пространстве, когда уже существует большой набор результатов. Менеджер баз данных динамически управляет памятью, используемой при размещении данных во временном дисковом пространстве.

Например, большой объем результатов может возникнуть при обработке устаревания данных. Если памяти системы недостаточно для хранения набора результатов, некоторые данные размещаются во временной дисковом пространстве. Если во время обработки устаревания выбран чрезмерно большой узел или файловое пространство, то менеджер баз данных не сможет отсортировать данные в памяти. Для сортировки данных менеджеру баз данных понадобится временное пространство.

Чтобы запустить операции базы данных, рассмотрите возможность добавления пространства базы данных для следующих сценариев:

- У базы данных маленький объем пространства, и операции сервера, которым требуется временное пространство, используют оставшуюся незанятую память.
- Файловые пространства велики, или для них назначена политика, которая создает много версий файлов.
- Сервер IBM Spectrum Protect должен быть запущен с ограниченным объемом памяти. Для запуска своих операций база данных использует главную память сервера IBM Spectrum Protect. Однако если памяти недостаточно, сервер IBM Spectrum Protect выделяет для базы данных временное пространство на диске. Например, если доступно 10 ГБ памяти, а для операций базы данных требуется 12 ГБ, база данных использует временное пространство.
- При внедрении сервера IBM Spectrum Protect появится сообщение об ошибке `недостаток памяти базы данных`. Отслеживайте в активном журнале сервера сообщения, относящиеся к пространству баз данных.

Важное замечание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами Fix Pack IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, чтобы не повредить базу данных.

Linux: Требования к пространству журнала восстановления

В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.

- Linux: Пространство активных и архивных журналов
  Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.
- Linux: Пространство зеркальной копии активного журнала
  Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.
- Linux: Пространство резервного архивного журнала
  Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Linux: Пространство активных и архивных журналов

Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.

Максимальный размер активного журнала для серверов IBM Spectrum Protect версии 7.1 и новее должен составлять 512 ГБ. Размер архивного журнала ограничен размером файловой системы, в которой он установлен.

Учитывайте следующие общие рекомендации для оценки размера активного журнала:

- Рекомендуемый начальный размер активного журнала - 16 Гбайт.
- Убедитесь, что размер активного журнала достаточен, по крайней мере, для тех текущих операций, которые обычно обрабатываются сервером. В качестве меры предосторожности попытайтесь учесть наибольший объем работы, которую сервер может выполнять единовременно. Обеспечьте для активного журнала некоторый дополнительный объем пространства, которое может использоваться при необходимости. Предусмотрите 20% дополнительного пространства.
- Отслеживайте используемое и доступное пространство активного журнала. При необходимости подстраивайте размер активного журнала в зависимости от таких факторов, как активность клиентов и уровень операций сервера.

- Убедитесь, что размер каталога, в котором содержится активный журнал, не меньше размера самого журнала. Если каталог больше по размеру, чем активный журнал, при необходимости он может использоваться для обработки аварийного восстановления.
- Убедитесь, что в файловой системе, которая содержит каталог активного журнала, есть по крайней мере 8 Гбайт свободного места для требований временных перемещений журналов.

Рекомендуемый начальный размер архивного журнала - 48 Гбайт.

Каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала, сгенерированные с момента последнего полного резервного копирования. Например, если вы производите резервное копирование базы данных ежедневно, каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала для всех операций клиентов в течение 24 часов. Чтобы освободить пространство, при полном резервном копировании базы данных сервер удаляет устаревшие файлы архивного журнала. Если каталог архивного журнала переполняется, а каталог резервного архивного журнала не существует, файлы журнала остаются в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением каталога активного журнала. При повторном запуске сервера часть используемого для активного журнала пространства освобождается.

После установки сервера вы можете отслеживать использование архивного журнала и пространство каталога архивного журнала. Если каталог архивного журнала переполняется, то это может привести к следующим проблемам:

- Сервер не сможет провести полное резервное копирование базы данных. Исследуйте и разрешите эту проблему.
- Другие приложения, выполняют запись в каталог архивного журнала, уменьшая объем доступного для архивного журнала пространства. Не используйте пространство архивного журнала для других прикладных программ, в том числе для других серверов IBM Spectrum Protect. Убедитесь, что у каждого сервера существует отдельное положение хранения, которым владеет и управляет данный сервер.

- Linux: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами
  Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.
- Linux: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов
  Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.
- Linux: Пример: оценка размера активного и архивного журналов для операций одновременной записи
  Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.
- Linux: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера
  Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.
- Linux: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности
  Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.
- Linux: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных
  Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.
- Linux: Пример: оценка размера активных и архивных журналов для операций дедупликации данных
  Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Linux: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами

Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.

Чтобы определить размеры активных и архивных журналов для основных операций сохранения, выполняемых клиентами, используйте следующую формулу:

```
число клиентов  x  число файлов, сохраненных в течение каждой транзакции
  x  размер пространства журнала, необходимый для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Основные операции сохранения данных клиентами

Элемент	**Значения примера**	**Описание**
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053 байта	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	19,5 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 байт = 3,5 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`3,5 + 16 = 19,5 ГБ`

Архивный журнал: Рекомендуемый размер	58,5 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала.
		
		`3,5 x 3 = 10,5 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`10,5 + 48 = 58,5 ГБ`

Элемент	Значения примера	Описание
[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.		

Linux: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов

Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.

Чтобы определить размеры активных и архивных журналов, когда клиенты используют несколько сеансов, примените следующую формулу:

```
число клиентов  x  число сеансов для каждого клиента  x  число файлов, сохраненных
  в течение каждой транзакции  x  объем памяти журнала, необходимой для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Несколько сеансов клиента

Элемент	Значения примера		Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	1000	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Возможных сеансов для каждого клиента	3	3	Параметр опции клиента RESOURCEUTILIZATION больше, чем значение по умолчанию. Каждый сеанс клиента запускает параллельно до трех сеансов.
Количество файлов, сохраняемых за каждую транзакцию	4096	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053	3053	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Элемент	Значения примера		Описание

Активный журнал: Рекомендуемый размер	26,5 ГБ [1]	51 ГБ [1]	Следующие вычисления проведены для 300 клиентов: Один гигабайт равен 1 073 741 824 байт.
			`(300 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 10,5 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`10,5 + 16 = 26,5 ГБ`
			Следующие вычисления проведены для 1000 клиентов: Один гигабайт равен 1 073 741 824 байт.
			`(1000 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 35 ГБ`
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			`35 + 16 = 51 ГБ`

Архивный журнал: Рекомендуемый размер	79,5 ГБ [1]	153 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
			`10,5 x 3 = 31,5 ГБ`
			`35 x 3 = 105 ГБ`
			Увеличим эти размеры на рекомендуемый начальный размер 48 ГБ:
			`31,5 + 48 = 79,5 ГБ`
			`105 + 48 = 153 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте ваш активный журнал и при необходимости настраивайте его размер.

Linux: Пример: оценка размера активного и архивного журналов для операций одновременной записи

Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.

Пространство журнала, требуемое для каждого файла, увеличивается примерно на 200 байт на каждый пул хранения копий, который используется для операции одновременной записи. В примере в следующей таблице данные сохраняются в двух пулах хранения копий в дополнение к первичному пулу хранения. Оценочный размер журнала увеличивается на 400 байт для каждого файла. Если использовать рекомендованное значение памяти журнала для каждого файла (3053 байта), полный объем составит 3453 байта.

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Одновременные операции записи

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байта на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3453 байта на каждый файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендуемый размер	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить требования к размеру архивного журнала:
		
		`4 ГБ x 3 = 12 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`12 + 48 = 60 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Linux: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций

сервера

Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.

Например, перемещение данных из дискового пула хранения с произвольным доступом (DISK) в дисковый пул хранения с последовательным доступом (FILE) использует примерно 110 байт памяти журнала на каждый перемещаемый файл. Допустим, например, что у вас есть 300 клиентов архивирования и резервного копирования, и каждый из них проводит резервное копирование 100 000 файлов каждую ночь. Файлы изначально хранятся в пуле хранения DISK, а затем переносятся в пул хранения FILE. Чтобы оценить объем памяти активного журнала, требуемой для этого перемещения данных, воспользуемся следующим вычислением. Число клиентов в формуле представляет собой максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время.

```
300 клиентов  x 100 000 файлов на каждого клиента  x  110 байт =  3,1 ГБ
```

Добавьте это значение к оценке размера активного журнала, полученной для основных операций сохранения данных клиентами.

Linux: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности

Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.

Linux: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных

Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.

Например, если полное резервное копирование базы данных производится раз в неделю, размер архивного журнала должен быть достаточным, чтобы содержать всю информацию за неделю в архивном журнале.

Различие в размерах архивного журнала для ежедневных и полных резервных копирований базы данных показано в примере в следующей таблице.

Табл. 1. Полное резервное копирование базы данных

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Элемент	Значения примера	Описание
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байт на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 файлов на транзакцию x 3453 байт на файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендованный размер при ежедневном полном резервном копировании базы данных	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
		
		`4 ГБ x 3 = 12 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`12 + 48 = 60 ГБ`

Архивный журнал: Рекомендованный размер при еженедельном полном резервном копировании базы данных	132 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала. Умножим этот результат на число дней между полными резервными копированиями базы данных:
		
		`(4 ГБ x 3 ) x 7 = 84 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`84 + 48 = 132 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Рекомендуемый начальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Linux: Пример: оценка размера активных и архивных журналов для операций дедупликации данных

Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Следующие факторы влияют на требования к размеру пространства активных и архивных журналов:

Объем дедуплицированных данных
: Влияние дедупликации данных на размер активного и архивного журналов зависит от процентной доли данных, которые могут использоваться для дедупликации. Если эта процентная доля данных для дедупликации относительно велика, потребуется больший объем пространства журналов.

Размер и количество экстентов
: Для каждого экстента, идентифицированного в процессе подготовки дедупликации, требуется примерно 1500 байт в пространстве активного журнала. Например, если при подготовке процесса дедупликации идентифицировано 250 тысяч экстентов, оценочный объем активного журнала составляет:

```
250 000 идентифицированных в каждом процессе экстентов x 1500 байт
 для каждого экстента = 358 МБ
```

Рассмотрим следующий сценарий: Триста клиентов архива резервных копий проводят каждую ночь до 100 тысяч операций резервного копирования файлов. Эти операции создают рабочую нагрузку в 30 миллионов файлов. Среднее количество экстентов для каждого файла - два. Следовательно, полное число экстентов - 60 миллионов, а для архивного журнала требуется 84 ГБ памяти:

```
60 000 000 экстентов x 1500 байт на каждый экстент = 84 ГБ
```

Процесс идентификации дубликатов оперирует с агрегатами файлов. Агрегат состоит из файлов, которые сохранены в данной транзакции, как задано опцией сервера TXNGROUPMAX. Предположим, что по умолчанию для опции сервера TXNGROUPMAX задано значение 4096. Если среднее число экстентов для каждого файла - два, общее число экстентов в каждом агрегате - 8192, а требуемая память активного журнала - 12 МБ:

```
8192 экстента в каждом агрегате x 1500 байт на каждый экстент =
   12 МБ
```

Время выполнения и число процессов идентификации дубликатов
: Время выполнения и число процессов идентификации дубликатов также влияют на размер активного журнала. Если использовать оцененный в предыдущем примере размер активного журнала (12 МБ), при параллельном выполнении десяти процессов идентификации дубликатов одновременная нагрузка активного журнала составит 120 МБ:

```
12 МБ на каждый процесс x 10 процессов = 120 МБ
```

Размер файла
: На размер активного журнала могут влиять также большие файлы, обрабатываемые для идентификации дубликатов. Допустим, например, что клиент резервного копирования и архивирования производит резервную копию около 80 гигабайтов (снимок файловой системы). В этом объекте может содержаться большое число дублированных экстентов, например, если проводилось инкрементное резервное копирование включенных в файловую систему файлов. Допустим, например, что снимок файловой системы содержит 1,2 миллиона дублированных экстентов. Эти 1,2 миллиона экстентов в таком большом файле представляют единственную транзакцию для процесса идентификации дубликатов. Требуемая для этого единственного объекта полная память активного журнала составляет 1,7 гигабайтов:

```
1 200 000 экстентов x 1500 байт на каждый экстент = 1,7 ГБ
```

Если одновременно с процессом идентификации дубликатов для этого большого объекта будет происходит аналогичный, но меньший по объему процесс, активному журналу может не хватить памяти. Допустим, например, что пул хранения включен для дедупликации. В пуле хранения содержится смесь данных, в том числе мелкие файлы с размером от 10 КБ до нескольких сотен КБ. В пуле хранения есть также несколько больших объектов, содержащих основную процентную долю дублированных экстентов.

Чтобы принять во внимание не только требования к объему памяти, но и затраты времени и продолжительность одновременных транзакций, увеличьте оцененный размер активного журнала примерно вдвое. Допустим, например, что ваша оценка дает для требуемого объема памяти значение 25 ГБ (23,3 ГБ + 1,7 ГБ на дедупликацию

большого объекта). Если процессы дедупликации выполняются одновременно, рекомендуемый размер активного журнала составит 50 ГБ. Предлагаемый размер архивного журнала - 150 ГБ.

Примеры в следующих таблицах показывают результаты расчетов для активных и архивных журналов. В примере первой таблицы использован средний размер экстента 700 КБ. Во втором примере (вторая таблица) средний размер экстента - 256 КБ. Как видно, меньший средний размер дубликата экстента (256 КБ) приводит к большему оцененному размеру активного журнала. Для исключения или минимизации проблем функционирования сервера используйте значение 256 КБ для оценки размера активного журнала в вашей производственной среде.

Табл. 1. Средний размер дубликата экстента - 700 КБ

Элемент	**Значения примера**		**Описание**
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	700 КБ	700 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.
Экстенты для данного файла	1 198 372 бит	6 135 667 бит	При использовании среднего размера экстентов (700 КБ) эта оценка дает среднее число экстентов для данного объекта. Для объекта размером 800 ГБ была использована следующая формула: `(800 ГБ ÷ 700 КБ) = 1 198 372 бит` Аналогичные вычисления для объекта размером 4 ТБ: `(4 ТБ ÷ 700 КБ) = 6 135 667`
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	1,7 ГБ	8,6 ГБ	Оценка размера активного журнала, требуемого для этой транзакции.

Элемент	Значения примера		Описание

Активный журнал: Рекомендуемый общий размер	66 ГБ [1]	79,8 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 1,7 ГБ) x 2 = 50 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`50 + 16 = 66 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 8,6 ГБ) x 2 = 63,8 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`63,8 + 16 = 79,8 ГБ`

Архивный журнал: Рекомендуемый размер	198 ГБ [1]	239,4 ГБ [1]	Увеличьте оцененный размер активного журнала втрое.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`50 ГБ x 3 = 150 ГБ`
			
			Увеличим этот размер на рекомендуемый начальный размер 48 ГБ:
			
			`150 + 48 = 198 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`63,8 ГБ x 3 = 191,4 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`191,4 + 48 = 239,4 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.			

Табл. 2. Средний размер дубликата экстента - 256 КБ

Элемент	Значения примера	Описание

Элемент	Значения примера		Описание
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	256 КБ	256 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.

Экстенты для данного файла	3 276 800 бит	16 777 216 бит	При использовании среднего размера экстентов эта оценка дает среднее число экстентов для данного объекта.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(800 ГБ ÷ 256 КБ) = 3 276 800 бит`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(4 ТБ ÷ 256 КБ) = 16 777 216 бит`

Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	4,5 ГБ	23,4 ГБ	Оценочный размер памяти активного журнала, требуемой для этой транзакции.

Активный журнал: Рекомендуемый общий размер	71,6 ГБ [1]	109,4 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 4,5 ГБ) x 2 = 55,6 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`55,6 + 16 = 71,6 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 23,4 ГБ) x 2 = 93,4 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`93,4 + 16 = 109,4 ГБ`

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	214,8 ГБ [1]	328,2 ГБ [1]	Троекратный размер оценки активного журнала.
			
			Следующие вычисления проведены для объекта размером 800 ГБ:
			
			`55,6 ГБ x 3 = 166,8 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`166,8 + 48 = 214,8 ГБ`
			
			Следующие вычисления проведены для объекта размером 4 ТБ:
			
			`93,4 ГБ x 3 = 280,2 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`280,2 + 48 = 328,2 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.			

Linux: Пространство зеркальной копии активного журнала

Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.

Создание зеркальной копии журнала - рекомендуемая опция. Если вы увеличите размер активного журнала, размер зеркальной копии журнала увеличится автоматически. Зеркальное копирование журнала может отрицательно сказаться на производительности, так как при зеркальном копировании потребуется удвоенный объем операций ввода-вывода. Дополнительное пространство, которое требуется для зеркальной копии журнала - это еще один фактор, который следует учесть, при принятии решения относительно создания зеркальной копии журнала.

Если каталог зеркальной копии журнала переполняется, сервер записывает сообщения об ошибке в активный журнал и в файл db2diag.log. Работа сервера продолжится.

Linux: Пространство резервного архивного журнала

Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Задав каталог резервного архивного журнала, можно предотвратить ошибки, которые могут происходить при нехватке места в каталоге архивного журнала. Если переполнятся и каталог архивного журнала, и диск или файловая система, где находится каталог резервного архивного журнала, данные останутся в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением активного журнала.

Linux: Мониторинг использования пространства для базы данных и журналов восстановления

Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.

Активный журнал

Если объем доступного пространства активного журнала недостаточен, в журнале операций появятся следующие записи:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Сервер IBM Spectrum Protect начинает полное резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Надо вручную выполнить резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
: Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Если должно будет начаться хотя бы одно полное резервное копирование базы данных, сервер IBM Spectrum Protect начнет инкрементное резервное копирование базы данных. В противном случае сервер начнет полное резервное копирование базы данных.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
: Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Надо вручную выполнить резервное копирование базы данных.

Архивный журнал

Если объем доступного пространства архивного журнала недостаточен, в журнале операций появится следующая запись:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
: Отношение размера используемого пространства архивного журнала к доступному размеру пространства архивного журнала превышает порог использования журнала. Сервер IBM Spectrum Protect начинает автоматическое полное резервное копирование базы данных.

Database

Если объем доступного пространства для операций базы данных недостаточен, в журнале операций появятся следующие сообщения:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
: Используемое пространство базы данных превышает порог использования пространства базы данных. Чтобы увеличить размер пространства для базы данных, используйте команду EXTEND DBSPACE, команду EXTEND DBSPACE или утилиту DSMSERV FORMAT с параметром DBDIR.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
: Размер доступного пространства в каталоге, где расположены серверные файлы базы данных, меньше 1 ГБ.

  Когда сервер IBM Spectrum Protect создается при помощи утилиты DSMSERV FORMAT или мастера по конфигурированию, одновременно создаются база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных. Указанный в этом сообщении каталог обозначает положение информации о базе данных, используемой менеджером баз данных. Если в этом каталоге нет доступного пространства, сервер больше не может функционировать.

  Необходимо добавить пространство к файловой системе или обеспечить доступное пространство в файловой системе или на диске.

Linux: Удаление файлов отката установки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Об этой задаче

Чтобы удалить файлы, которые больше не нужны, используйте либо графический мастер установки, либо командную строку в режиме консоли.

- Linux: Удаление файлов отката установки с использованием графического мастера
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.
- Linux: Удаление файлов отката установки с использованием командной строки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Linux: Удаление файлов отката установки с использованием графического мастера

Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.

Процедура

1. Откройте IBM Installation Manager.
    Операционные системы LinuxВ каталоге, в котором установлен IBM Installation Manager, перейдите в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду, чтобы запустить IBM Installation Manager:

   ```
   ./IBMIM
   ```

2. Щелкните по Файл > Предпочтения.
3. Выберите Файлы для отката.
4. Щелкните по Удалить сохраненные файлы и нажмите на OK.

Linux: Удаление файлов отката установки с использованием командной строки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Процедура

1. В каталоге, в котором установлен IBM® Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы Linuxeclipse/tools

   Например:

   -  Операционные системы Linux/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду, чтобы запустить командную строку IBM Installation Manager:
   -  Операционные системы Linux`./imcl -c`
3. Введите `П`, чтобы выбрать Предпочтения.
4. Введите `3`, чтобы выбрать Файлы для отката.
5. Введите `D`, чтобы удалить файлы для отката.
6. Введите `A`, чтобы применить изменения и вернуться в меню предпочтений.
7. Введите `C`, чтобы выйти из Меню предпочтений.
8. Введите `X`, чтобы закрыть Installation Manager.

Linux: Практические рекомендации по именованию сервера

Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.

ID пользователя экземпляра

ID пользователя экземпляра служит основой для других имен, связанных с экземпляром сервера. ID пользователя экземпляра также называют владельцем экземпляра.

Например: tsminst1

ID пользователя экземпляра - это ID пользователя, у которого должны быть полномочия владельца или доступ с правом на чтение/запись для всех каталогов, которые вы создаете для базы данных и журнала восстановления. Обычная практика работы сервера - его запуск от имени ID пользователя экземпляра. У этого ID пользователя должно быть право чтения и записи в каталоги, используемые для всех классов устройств FILE.

 Операционные системы Linux

Домашний каталог для ID пользователя экземпляра

Домашний каталог (если он еще не существует) можно создать при создании ID пользователя экземпляра, указав для этого опцию -m. В зависимости от локальных параметров имя домашнего каталога может иметь следующий вид: /home/*ID_пользователя_экземпляра*.

Например: /home/tsminst1

Домашний каталог изначально используется для содержания профиля ID пользователя и параметров безопасности.

 Операционные системы Linux

Имя экземпляра базы данных

Имя экземпляра базы данных должно совпадать с ID пользователя экземпляра, от имени которого вы запускаете экземпляр сервера.

Например: tsminst1

 Операционные системы Linux

Каталог экземпляра

Каталог экземпляра - это каталог, содержащий связанные с экземпляром сервера файлы (файл опций сервера и другие специфичные для сервера файлы). У этого каталога может быть любое имя по вашему выбору. Чтобы этот каталог было проще распознать, используйте имя, связывающее каталог с именем экземпляра.

Каталог экземпляра можно создать как подкаталог домашнего каталога ID пользователя экземпляра. Например: /home/*ID_пользователя_экземпляра*/*ID_пользователя_экземпляра*

В приведенном ниже примере каталог экземпляра размещается в домашнем каталоге для пользователя с ID tsminst1: /home/tsminst1/tsminst1

Этот каталог также можно создать в другом месте, например: /tsmserver/tsminst1

В каталоге экземпляра хранятся следующие файлы для экземпляра сервера:

- Файл серверных опций, dsmserv.opt
- Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
- Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
- Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
- Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.
- Обработчики пользователя
- Выходная информация трассировки (если не задано полное имя)

Имя базы данных

Именем базы данных для каждого экземпляра сервера всегда является TSMDB1. Это имя нельзя изменить.

Имя сервера

Имя сервера - это внутреннее имя для IBM Spectrum Protect, и оно используется для выполнения операций, включающих в себя взаимодействия между несколькими серверами IBM Spectrum Protect. В качестве примера можно привести взаимодействие сервера с сервером и совместное использование библиотеки.

 Операционные системы LinuxИмя сервера также используется при добавлении сервера в Центр операций, чтобы им можно было управлять с использованием этого интерфейса. Используйте для каждого сервера уникальное имя. Чтобы имя было проще распознать в Центре операций или в выходной информации команды QUERY SERVER, используйте имя, отражающее положение или назначение сервера. Не изменяйте имя сервера IBM Spectrum Protect после того, как он сконфигурирован как хаб или подчиненный сервер.

Если вы используете мастер, рекомендуемым именем по умолчанию будет имя хоста компьютера, который вы используете. Можно использовать другое имя, которое будет иметь смысл в вашей среде. Если у вас в системе более одного сервера и вы используете мастер, вы сможете использовать имя по умолчанию только для одного из серверов. Для каждого сервера нужно ввести уникальное имя.

 Операционные системы LinuxНапример:

- `PAYROLL`
- `SALES`

Каталоги для пространства базы данных и журнала восстановления

Каталогам можно присваивать имена в соответствии с принятой у вас практикой. Чтобы было проще распознавать каталоги, используйте имена, связывающие каталоги с экземпляром сервера.

Например, в случае архивного журнала:

-  Операционные системы Linux/tsminst1_archlog

Linux: Каталоги установки

К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

(/opt/tivoli/tsm/server/bin) - это каталог по умолчанию, содержащий код сервера и файлы лицензии.

Структура каталогов продукта DB2, устанавливаемого в ходе установки сервера IBM Spectrum Protect, соответствует тому, что задокументировано в источниках информации по DB2. Защищайте эти каталоги и файлы так же, как вы защищаете каталоги сервера. Каталог по умолчанию - /opt/tivoli/tsm/db2.

Можно использовать следующий языки: английский (США), испанский, итальянский, китайский Big5, китайский GBK, китайский традиционный, китайский упрощенный, корейский, немецкий, португальский (Бразилия), русский, французский и японский.

Linux: Установка компонентов сервера

Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.

Об этой задаче

При использовании программы установки IBM Spectrum Protect можно установить следующие компоненты:

- сервер (server)
  Совет: База данных (DB2), Global Security Kit (GSKit) и IBM® Java™ Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- языки сервера
- лицензия
- устройства
- IBM Spectrum Protect for SAN

- Центр операций

Операционные системы LinuxДля установки сервера версии 8.1.5 надо выделить примерно 30 - 45 минут.

- Linux: Получение пакета установки
  Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM (например, Passport Advantage или IBM Fix Central).
- Linux: Установка IBM Spectrum Protect при помощи мастера установки
  Сервер можно установить при помощи графического мастера IBM Installation Manager.
- Linux: Установка IBM Spectrum Protect в режиме консоли
  IBM Spectrum Protect можно установить из командной строки в режиме консоли.
- Linux: Установка IBM Spectrum Protect в режиме без вывода сообщений
  Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.
- Linux: Установка языковых пакетов сервера
  Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Linux: Получение пакета установки

Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM® (например, Passport Advantage или IBM Fix Central).

Операционные системы Linux

Прежде чем начать

Если вы собираетесь скачать эти файлы, задайте неограниченный системный предел пользователя для максимального размера файла, чтобы файлы были успешно скачаны:

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

   ```
   ulimit -Hf
   ```

2. Если системный пользовательский предел на максимальный размер файла не задан неограниченным, измените его на неограниченный, следуя инструкциям в документации для вашей операционной системы.

Процедура

1. Загрузите нужный файл пакета с одного из следующих веб-сайтов.
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.
   - Самую свежую информацию, обновления и исправления обслуживания смотрите по адресу: Портал поддержки IBM.
2. Если вы скачали пакет с сайта скачивания IBM, то сделайте следующее:
   Операционные системы Linux
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к свободному месту можно увидеть в документе по скачиванию:
      - IBM Spectrum Protect техническое замечание 4042944
      - IBM Spectrum Protect Extended Edition техническое замечание 4042945
      - IBM Spectrum Protect for Data Retention техническое замечание 4042946

   b. Скачайте файл пакета в каталог по вашему выбору. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.
   c. Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

      ```
      chmod a+x имя_пакета.bin
      ```

   d. Извлеките пакет, введя следующую команду:

      ```
      ./имя_пакета.bin
      ```

      где *имя_пакета* - это имя скачанного файла, например:

Операционные системы Linux

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Выберите один из следующих способов установки IBM Spectrum Protect:
   - Linux: Установка IBM Spectrum Protect при помощи мастера установки
   - Linux: Установка IBM Spectrum Protect в режиме консоли
   - Linux: Установка IBM Spectrum Protect в режиме без вывода сообщений
4. После установки IBM Spectrum Protect и до настройки этого продукта в соответствии с вашими требованиями посетите следующий веб-сайт: Портал поддержки IBM. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Linux: Установка IBM Spectrum Protect при помощи мастера установки

Сервер можно установить при помощи графического мастера IBM® Installation Manager.

Прежде чем начать

Перед запуском установки сделайте следующее:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки, введя следующую команду: Операционные системы Linux `./install.sh`

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Вы можете просмотреть файлы журнала установки, выбрав Файл > Просмотреть журнал в инструменте Installation Manager. Чтобы выполнить сбор этих файлов журнала, выберите Справка > Экспорт данных для анализа проблем в инструменте Installation Manager.

- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.

- Операционные системы LinuxПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

Linux: Установка IBM Spectrum Protect в режиме консоли

IBM Spectrum Protect можно установить из командной строки в режиме консоли.

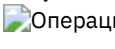
Прежде чем начать

Перед запуском установки сделайте следующее:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки в консольном режиме, введя следующую команду:  Операционные системы Linux `./install.sh -c` Необязательно: Сгенерируйте файл ответов в ходе установки в режиме консоли. Укажите опции установки в режиме консоли и на панели Сводка укажите `G`, чтобы сгенерировать ответы.

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  -  Операционные системы Linux/var/ibm/InstallationManager/logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
-  Операционные системы LinuxПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

Linux: Установка IBM Spectrum Protect в режиме без вывода сообщений

Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге input в том месте, куда был распакован пакет установки:

install_response_sample.xml
: Используйте этот файл для установки компонентов IBM Spectrum Protect.

update_response_sample.xml
: Используйте этот файл для обновления компонентов IBM Spectrum Protect.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов. Вы можете изменить пример файла ответов или создать свой собственный.
2. Если вы устанавливаете сервер и компонент Центр операций в режиме без вывода сообщений, создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.
   Если вы используете файл install_response_sample.xml, добавьте пароль в следующую строку в файле, где *пароль* - это пароль:

   ```
   <variable name='ssl.password' value='пароль' />
   ```

Дополнительную информацию об этом пароле смотрите в разделе Контрольный список установки.
Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл update_response_sample.xml для обновления компонента Центр операций.

3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:
   - Операционные системы Linux

```
./install.sh -s -input файл_ответов
-acceptLicense
```

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  - Операционные системы Linux/var/ibm/InstallationManager/logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
- Операционные системы LinuxПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.

Операционные системы Linux

Linux: Установка языковых пакетов сервера

Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Прежде чем начать

Инструкции по установке пакетов поддержки национальных языков для агента хранения смотрите в документе Конфигурация пакета поддержки национальных языков для агентов хранения.

- Linux: Локали языка сервера
  Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.
- Linux: Конфигурирование языкового пакета
  После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.
- Linux: Обновление языкового пакета
  Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

Linux: Локали языка сервера

Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.

Операционные системы LinuxЭтот языковый пакет автоматически устанавливается для следующей языковой опции по умолчанию для сообщений и справки сервера IBM Spectrum Protect:

- Операционные системы LinuxLANGUAGE en_US

Для прочих языков и локалей установите языковой пакет, нужный для вашей установки.
Можно использовать следующие языки:
Операционные системы Linux

Табл. 1. Языки сервера для Linux

LANGUAGE	Значение опции LANGUAGE
Китайский упрощенный	zh_CN
	zh_CN.gb18030

LANGUAGE	Значение опции LANGUAGE
	zh_CN.utf8
Китайский традиционный	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Английский, США	en_US
	en_US.utf8
Французский	fr_FR
	fr_FR.utf8
Немецкий	de_DE
	de_DE.utf8
Итальянский	it_IT
	it_IT.utf8
Японский	ja_JP
	ja_JP.utf8
Корейский	ko_KR
	ko_KR.utf8
Бразильский португальский	pt_BR
	pt_BR.utf8
Русский	ru_RU
	ru_RU.utf8
Испанский	es_ES
	es_ES.utf8

 Операционные системы LinuxОграничение: При использовании Центр операций некоторые символы могут выводиться неправильно, если язык веб-браузера не совпадает с языком сервера. При появлении этой неполадки следует сконфигурировать в браузере использование того же языка, что и на сервере.

Linux: Конфигурирование языкового пакета

После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.

Об этой задаче

 Операционные системы LinuxДля задания поддержки определенной локали выполните одну из следующих задач:

- Для опции LANGUAGE в файле опций сервера задайте имя локали, которую нужно использовать. Например:
  -  Операционные системы LinuxЧтобы использовать локаль `ru_RU.UTF-8`, задайте для опции LANGUAGE значение `ru_RU.UTF-8`. Смотрите раздел Linux: Локали языка сервера.
-  Операционные системы LinuxЕсли вы запускаете сервер в режиме активного окна, то задайте для переменной среды `LC_ALL` значение, совпадающее со значением, которое задано в файле опций сервера. Например, чтобы задать переменную среды для русского языка, введите следующее значение:

  ```
  export LC_ALL=ru_RU.UTF-8
  ```

Если локаль успешно инициализирована, то с ее помощью форматируется дата, время и представление чисел для сервера. Если локаль не инициализируется успешно, сервер будет использовать файлы сообщений на английском языке (США), а также формат дат времени и чисел для языка системы 'Английский (США)'.

Linux: Обновление языкового пакета

Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

Об этой задаче

Внутри одного и того же экземпляра IBM Spectrum Protect можно установить другой языковой пакет.

- Для установки другого языкового пакета используйте функцию Изменить программы IBM Installation Manager.
- Для обновления языковых пакетов до новых версий используйте функцию Обновить программы IBM Installation Manager.

Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* являются синонимами.

Linux: Первые шаги после установки IBM Spectrum Protect

После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.

Об этой задаче

1. Операционные системы LinuxИзмените значения параметров ядра.

   Операционные системы LinuxСмотрите раздел Linux: Настройка параметров ядра для систем Linux.

2. Создайте каталоги и ID пользователя для экземпляра сервера. Смотрите раздел Linux: Создание ID пользователя и каталогов для экземпляра сервера.
3. Сконфигурируйте экземпляр сервера. Выберите одну из следующих опций.
   - Воспользуйтесь мастером по конфигурированию - это рекомендуемый способ. Смотрите раздел Linux: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования.
   - Сконфигурируйте вручную новый экземпляр. Смотрите раздел Linux: Конфигурирование экземпляра сервера вручную. При конфигурировании вручную выполните описанные ниже шаги.
     a. Сконфигурируйте каталоги и создайте экземпляр IBM Spectrum Protect. Смотрите раздел Linux: Создание экземпляра сервера.
     b. Создайте новый файл серверных опций, скопировав пример файла, чтобы сконфигурировать связь между сервером и клиентами. Смотрите раздел Операционные системы LinuxLinux: Конфигурирование связи между сервером и клиентом.
     c. Введите команду DSMSERV FORMAT, чтобы сформатировать базу данных. Смотрите раздел Linux: Форматирование базы данных и журнала.
     d. Сконфигурируйте систему для резервного копирования базы данных. Смотрите раздел Linux: Подготовка менеджера базы данных к резервному копированию базы данных.
4. Сконфигурируйте опции, чтобы задать, когда запускать реорганизацию базы данных. Смотрите раздел Linux: Опции конфигурирования сервера для обслуживания сервера баз данных.
5. Запустите экземпляр сервера, если он еще не запущен.
   - Операционные системы LinuxСмотрите раздел Linux: Запуск экземпляра сервера.
6. Зарегистрируйте свою лицензию. Смотрите раздел Linux: Регистрация лицензий.
7. Подготовьте систему для резервного копирования базы данных. Смотрите раздел Linux: Подготовка сервера к операциям резервного копирования базы данных.
8. Наблюдайте сервер. Смотрите раздел Linux: Мониторинг сервера.

- Операционные системы LinuxLinux: Настройка параметров ядра для систем Linux
  Для правильной установки и работы IBM Spectrum Protect и DB2 в Linux надо изменить параметры конфигурации ядра.
- Linux: Создание ID пользователя и каталогов для экземпляра сервера
  Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.
- Linux: Конфигурирование сервера IBM Spectrum Protect
  После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.
- Linux: Опции конфигурирования сервера для обслуживания сервера баз данных
  Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный

режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

- Операционные системы LinuxLinux: Запуск экземпляра сервера
  Сервер можно запускать от имени ID пользователя экземпляра (что является предпочтительным методом) или от имени ID пользователя root.
- Linux: Остановка сервера
  При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.
- Linux: Регистрация лицензий
  Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.
- Linux: Подготовка сервера к операциям резервного копирования базы данных
  Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.
- Linux: Запуск нескольких экземпляров серверов на одном компьютере
  Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.
- Linux: Мониторинг сервера
  Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Операционные системы Linux

Linux: Настройка параметров ядра для систем Linux

Для правильной установки и работы IBM Spectrum Protect и DB2 в Linux надо изменить параметры конфигурации ядра.

Об этой задаче

Если вы не измените эти параметры, установка DB2 и IBM Spectrum Protect может завершиться неудачно. И даже при успешной установке при работе могут возникнуть проблемы.

- Операционные системы LinuxLinux: Изменение параметров ядра в Linux
  DB2 автоматически увеличивает значения параметров ядра межпроцессовой связи (interprocess communication, IPC) до предпочтительных.
- Операционные системы LinuxLinux: Рекомендуемые значения для параметров ядра в Linux
  Убедитесь, что значения параметров ядра достаточны для исключения проблем при работе сервера IBM Spectrum Protect.

Операционные системы Linux

Linux: Изменение параметров ядра в Linux

DB2 автоматически увеличивает значения параметров ядра межпроцессовой связи (interprocess communication, IPC) до предпочтительных.

Об этой задаче

Чтобы изменить параметры ядра на сервере Linux, выполните следующие действия:

Процедура

1. Введите команду ipcs -l, чтобы вывести список значений параметров.
2. Проанализируйте результаты, чтобы определить, требуются ли какие-либо изменения для вашей системы. Если требуются изменения, можно задать параметр в файле /etc/sysctl.conf. Это значение параметра применяется при запуске системы.

Дальнейшие действия

Для Red Hat Enterprise Linux 6 (RHEL6) надо задать параметр `kernel.shmmax` в файле /etc/sysctl.conf до автоматического перезапуска сервера IBM Spectrum Protect при запуске системы.

Подробную информацию о базе данных DB2 для Linux смотрите по адресу: Информация о DB2.

 Операционные системы Linux

Linux: Рекомендуемые значения для параметров ядра в Linux

Убедитесь, что значения параметров ядра достаточны для исключения проблем при работе сервера IBM Spectrum Protect.

Об этой задаче

В следующей таблице приводятся рекомендуемые параметры ядра для запуска как IBM Spectrum Protect, так и DB2.

Параметр	Описание	Рекомендуемое значение
kernel.randomize_va_space	Параметр kernel.randomize_va_space конфигурирует использование ядром памяти ASLR. Если вы задаете значение 0, `kernel.randomize_va_space=0`, ASLR отключается. Серверы данных DB2 рассчитывают на фиксированные адреса для определенных объектов совместно используемой памяти, и ASLR может вызывать ошибки при некоторых операциях. Дополнительные подробности об ASLR Linux и DB2 смотрите в техническом замечании по адресу: http://www.ibm.com/support/docview.wss?uid=swg21365583.	0
vm.swappiness	Параметр vm.swappiness определяет, может ли ядро выполнять своппинг для памяти программы из физической оперативной памяти. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.	0
vm.overcommit_memory	Параметр vm.overcommit_memory влияет на то, какой объем виртуальной памяти ядро позволяет размещать. Дополнительную информацию о параметрах ядра смотрите по адресу Информация о DB2.	0

Linux: Создание ID пользователя и каталогов для экземпляра сервера

Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.

Прежде чем начать

Прежде чем выполнять данную задачу, ознакомьтесь с информацией о планировании пространства для сервера. Смотрите раздел Linux: Контрольные списки для планирования сведений о сервере.

Процедура

1. Создайте ID пользователя, который станет владельцем экземпляра сервера. Вы будете использовать этот ID пользователя при создании экземпляра сервера в одном из последующих шагов.

    Операционные системы Linux

Операционные системы LinuxСоздайте ID пользователя и группу, которые станут владельцем экземпляра сервера.

a. От имени ID пользователя - администратора можно запустить следующие команды конфигурирования пользователей и групп. Создайте ID пользователя и группу в домашнем каталоге пользователя. Ограничение: В ID пользователя можно использовать буквы нижнего регистра (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя и имя группы должны соответствовать следующим правилам:
   - Длина не должна превышать 8 символов.
   - ID пользователя не может начинаться с *ibm*, *sql*, *sys* или цифры.
   - В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

   Например, создайте ID пользователя `tsminst1` в группе `tsmsrvrs`. В приведенных ниже примерах показано, как создать этот ID пользователя и эту группу при помощи команд операционной системы.

   Операционные системы Linux

   ```
   groupadd tsmsrvrs -g 1111
   useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
   passwd tsminst1
   ```

   Ограничение: DB2 не поддерживает непосредственную аутентификацию пользователя системы через LDAP.

b. Выйдите из системы, затем снова в нее войдите. Перейдите на только что созданную учетную запись пользователя. Используйте интерактивную программу входа в систему, например, telnet, чтобы вас попросили ввести пароль и вы смогли изменить его, если это потребуется.

2. Создайте каталоги, необходимые серверу.
   Операционные системы LinuxСоздайте пустые каталоги для каждого элемента в таблице и убедитесь, что каталогами владеет новый ID пользователя, который вы только что создали. Смонтируйте связанную систему хранения каждому каталогу для активного и архивного журнала, а также для каталогов базы данных.

Элемент	**Примеры команд для создания каталогов**	**Ваши каталоги**
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)	`mkdir /tsminst1`	

Каталоги базы данных	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Каталог активного журнала	`mkdir /tsmlog`	
Каталог архивного журнала	`mkdir /tsmarchlog`	
Необязательно: Каталог для зеркальной копии активного журнала	`mkdir /tsmlogmirror`	
Необязательно: Каталог вторичного архивного журнала (каталог для резервного архивного журнала)	`mkdir /tsmarchlogfailover`	

   При первоначальном создании сервера при помощи утилиты DSMSERV FORMAT или мастера конфигурирования создается база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных.

3. Завершите сеанс для нового ID пользователя.

Linux: Конфигурирование сервера IBM Spectrum Protect

После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.

Об этой задаче

Сконфигурируйте экземпляр сервера IBM Spectrum Protect, выбрав один из следующих вариантов:

- Linux: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования
  Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.
- Linux: Конфигурирование экземпляра сервера вручную
  После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

Linux: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования

Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.

Прежде чем начать

Прежде чем использовать мастер конфигурирования, нужно выполнить все предыдущие шаги для подготовки к конфигурированию. В число этих шагов входят установка IBM Spectrum Protect, создание каталогов базы данных и журналов и создание каталогов и ID пользователя для экземпляра сервера.

Процедура

1. Убедитесь, что выполнены следующие требования:
    Операционные системы Linux
   - В системе, в которой вы установили IBM Spectrum Protect, должен быть клиент X Window System. Кроме того, у вас на рабочем столе должен работать сервер X Window System.
   - В системе должен быть разрешен протокол Secure Shell (SSH). Убедитесь, что для порта задано значение по умолчанию (22) и что порт не заблокирован брандмауэром. Нужно разрешить аутентификацию пароля в файле `sshd_config` в каталоге /etc/ssh/. Убедитесь также, что у службы демона SSH есть права доступа для соединения с системой с использованием значения `localhost`.
   - Вы должны иметь возможность войти в систему, используя ID пользователя, созданный для экземпляра сервера, и протокол SSH. При использовании мастера для получения доступа к системе вы должны будете ввести эти ID пользователя и пароль.
   - Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
     - Файлы главного ключа шифрования (`dsmkeydb.*`)
     - Сертификат сервера и файлы секретных ключей (`cert.*`)

2. Запустите локальную версию мастера:
   -  Операционные системы LinuxОткройте программу `dsmicfgx` в каталоге /opt/tivoli/tsm/server/bin. Этот мастер можно запускать только с использованием ID пользователя root.

   Завершите конфигурирование, следуя инструкциям. Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

Linux: Конфигурирование экземпляра сервера вручную

После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

- Linux: Создание экземпляра сервера
  Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.
- Операционные системы LinuxLinux: Конфигурирование связи между сервером и клиентом
  Пример файла серверных опций по умолчанию, dsmserv.opt.smp, создается в каталоге /opt/tivoli/tsm/server/bin при установке IBM Spectrum Protect. Вы должны сконфигурировать связь между сервером и клиентами, создав новый файл серверных опций. Для этого скопируйте пример файла в каталог экземпляра сервера.
- Linux: Форматирование базы данных и журнала
  Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.
- Linux: Подготовка менеджера базы данных к резервному копированию базы данных
  Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Linux: Создание экземпляра сервера

Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.

Об этой задаче

На одной рабочей станции может быть один или несколько экземпляров сервера.
Операционные системы LinuxВажное замечание: Прежде чем вводить команду db2icrt, убедитесь в следующем:

- Существует домашний каталог для пользователя (/home/tsminst1). Если домашнего каталога нет, вы должны его создать.
  В каталоге экземпляра хранятся следующие файлы, сгенерированные сервером IBM Spectrum Protect:
  - Файл серверных опций, dsmserv.opt
  - Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
  - Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
  - Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
  - Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.
  - Обработчики пользователя
  - Выходная информация трассировки (если не задано полное имя)
- Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
  - Файлы главного ключа шифрования (`dsmkeydb.*`)
  - Сертификат сервера и файлы секретных ключей (`cert.*`)
- У пользователя root и ID пользователя экземпляра должны быть разрешения на запись в файл конфигурации оболочки. В домашнем каталоге существует файл конфигурации оболочки (например, .profile). Дополнительную информацию смотрите на веб-сайте Информация о DB2. Найдите информацию о переменных среды Linux и UNIX.

Операционные системы Linux

1. Войдите в систему с ID пользователя root и создайте экземпляр IBM Spectrum Protect. Имя экземпляра должно совпадать с именем пользователя, являющегося владельцем экземпляра. Введите команду db2icrt в виде одной строки:Операционные системы Linux

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   имя_экземпляра имя_экземпляра
   ```

   Например, если ID пользователя данного экземпляра - tsminst1, создайте экземпляр, введя следующую команду:
   Введите команду в одной строке.Операционные системы Linux

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Напоминание: С этого момента используйте этот новый ID пользователя при конфигурировании сервера IBM Spectrum Protect. Завершите сеанс ID пользователя root и войдите в систему от имени нового ID пользователя-владельца экземпляра.
2. Измените каталог по умолчанию для базы данных, так чтобы он совпадал с каталогом экземпляра сервера. Если у вас несколько серверов, войдите в систему от имени ID пользователя экземпляра для каждого сервера. Введите команду:

```
db2 update dbm cfg using dftdbpath каталог_экземпляра
```

Например, если значением каталог_экземпляра является ID пользователя экземпляра:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Измените путь библиотеки, включив в него библиотеки, необходимые для операций сервера.
   Совет: В следующих примерах используются следующие каталоги:
   - *каталог_bin_сервера* - это подкаталог каталога установки сервера. Например, /opt/tivoli/tsm/server/bin.
   - *домашний_каталог_пользователей_экземпляра* - это домашний каталог пользователя экземпляра. Например, /home/tsminst1.

   .
   - Надо изменить один из следующих файлов, чтобы задать путь библиотек, когда запускаются DB2 или сервер. Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

     Оболочка Bash или Korn:

     ```
     домашний_каталог_пользователей_экземпляра/sqllib/userprofile
     ```

     Оболочка C:

     ```
     домашний_каталог_пользователей_экземпляра/sqllib/usercshrc
     ```

   - Произведите обновление для оболочки, для использования которой сконфигурирован экземпляр пользователя.

     Оболочка Bash или Korn:

     Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/userprofile следующую запись (в одной строке):Операционные системы Linux

     ```
     export LD_LIBRARY_PATH=каталог_bin_сервера/
     dbbkapi:/usr/local/ibm/gsk8_64/lib64:/opt/ibm/lib:/opt/
     ibmlib64:$LD_LIBRARY_PATH
     ```

     Оболочка C:

     Добавьте в файл *домашний_каталог_пользователей_экземпляра*/sqllib/usercshrc следующую запись (на одной строке):Операционные системы Linux

     ```
     setenv LD_LIBRARY_PATH каталог_bin_сервера/dbbkapi:/
     usr/local/ibm/gsk8_64/lib64:/
     opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
     ```

     Напоминание: В пути библиотек должны быть следующие записи, и они должны идти перед всеми другими записями в пути библиотек:
     - каталог_bin_сервера/dbbkapi
     - /usr/local/ibm/gsk8_64/lib64
4. Создайте новый файл серверных опций. Смотрите раздел Linux: Конфигурирование связи между сервером и клиентом.

Операционные системы Linux

Linux: Конфигурирование связи между сервером и клиентом

Пример файла серверных опций по умолчанию, dsmserv.opt.smp, создается в каталоге /opt/tivoli/tsm/server/bin при установке IBM Spectrum Protect. Вы должны сконфигурировать связь между сервером и клиентами, создав новый файл серверных опций. Для этого скопируйте пример файла в каталог экземпляра сервера.

Об этой задаче

Убедитесь, что у вас есть каталог экземпляра сервера, например, /tsminst1, и скопируйте в него файл примера. Присвойте новому файлу имя `dsmserv.opt` и измените опции. Выполните это действие до инициализации базы данных сервера. Каждый образец записи или запись по умолчанию в стандартном файле опций является примечанием - строкой, начинающейся со звездочки (*). Регистр символов в именах опций не имеет значения, а между ключевыми словами и значениями можно вставлять один или несколько пробелов.

При изменении файла опций соблюдайте следующие рекомендации.

- Для активации опции удалите звездочку в начале строки.
- Для ввода опций можно использовать любой столбец.
- Одна строка должна содержать только одну опцию, а одна опция должна занимать только одну строку.
- Если одному ключевому слову соответствует несколько записей, сервер IBM Spectrum Protect использует последнюю запись.

При внесении изменений в файл опций сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Можно задать один из следующих методов связи:

- TCP/IP версии 4 или версии 6
- Совместное использование памяти
- Secure Sockets Layer (SSL)
  Совет: Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера IBM Spectrum Protect. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

-  Операционные системы LinuxLinux: Задание опций TCP/IP
  Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.
-  Операционные системы LinuxLinux: Задание опций Shared Memory
  Вы можете использовать связь через совместную память (Shared Memory) для взаимодействия между клиентами и серверами на одном и том же компьютере. Чтобы использовать способ связи Shared Memory, в системе должен быть установлен протокол TCP/IP версии 4.
-  Операционные системы LinuxLinux: Задание опций Secure Sockets Layer
  Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Linux: Задание опций TCP/IP

Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.

Об этой задаче

Ниже приводится пример списка опций TCP/IP, которые вы можете использовать для конфигурирования системы.

```
commmethod         tcpip
  tcpport            1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Совет: Можно использовать протокол TCP/IP версии 4, версии 6 или обеих версий.

TCPPORT
: Адрес порта сервера для взаимодействий TCP/IP и SSL. Значение по умолчанию - 1500.

 Операционные системы LinuxTCPWINDOWSIZE
:  Операционные системы LinuxЗадает размер буфера TCP/IP, используемого при отправке или приеме данных. Размер окна, используемого в сеансе, меньше размера окна для сервера и клиента. При большем размере окна используется дополнительная память, но это может способствовать повышению производительности.

  Можно задать целое число от 0 до 2048. Чтобы использовать размер окна по умолчанию для операционной системы, задайте значение 0.

TCPNODELAY
: Позволяет указать, будет ли сервер отправлять сообщения малого объема, или же он разрешит TCP/IP буферизовать сообщения. При отправке небольших сообщений может повыситься пропускная способность, но при этом увеличится число пакетов, отправляемых по сети. Укажите YES, чтобы отправлять короткие сообщения, или NO, чтобы протокол TCP/IP сохранял их в буфере. Значение по умолчанию - YES.

TCPADMINPORT
: Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований связи с поддержкой TCP/IP или SSL, отличных от сеансов клиентов. Значением по умолчанию является значение TCPPORT.

SSLTCPPORT
: (Только SSL) Задает номер порта Secure Sockets Layer (SSL), на котором драйвер связи TCP/IP ожидает запросы на установление сеансов SSL от клиента резервного копирования и архивирования и клиента администрирования с

интерфейсом командной строки.

SSLTCPADMINPORT

(Только SSL) Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает запросов на установление сеансов SSL от клиента администрирования с интерфейсом командной строки.

Linux: Задание опций Shared Memory

Вы можете использовать связь через совместную память (Shared Memory) для взаимодействия между клиентами и серверами на одном и том же компьютере. Чтобы использовать способ связи Shared Memory, в системе должен быть установлен протокол TCP/IP версии 4.

Об этой задаче

В приведенном ниже примере показан параметр для совместно используемой памяти (shared memory):

```
commmethod      sharedmem
   shmport      1510
```

В этом примере SHMPORT задает адрес порта TCP/IP для сервера при связи через совместно используемую память. Опцию SHMPORT можно использовать, чтобы задать другой порт TCP/IP. По умолчанию используется порт 1510. COMMMETHOD можно использовать несколько раз в файле опций сервера IBM Spectrum Protect с различными значениями. Например, можно задать значения так:

```
commmethod         tcpip
commmethod      sharedmem
```

 Операционные системы LinuxПри использовании связи через совместную память вы можете получить от сервера следующее сообщение:

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error from msgget (2), errno = 28
```

Это сообщение означает, что необходимо создать очередь сообщений, но при этом будет превышено максимально допустимое число очередей сообщений (MSGMNI).

 Операционные системы LinuxЧтобы узнать максимальное число очередей сообщений (MSGMNI) в системе, введите следующую команду:

```
cat /proc/sys/kernel/msgmni
```

Чтобы увеличить значение MSGMNI в системе, введите следующую команду:

```
sysctl -w kernel.msgmni=n
```

где **n** - максимальное число очередей сообщений в системе (MSGMNI), которое вы хотите задать.

Linux: Задание опций Secure Sockets Layer

Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Прежде чем начать

SSL — это стандартная технология создания зашифрованных сеансов между серверами и клиентами. SSL предоставляет безопасный канал для связи серверов и клиентов по открытым путям связи. При использовании SSL идентификационная информация сервера проверяется с помощью цифровых сертификатов.

Чтобы обеспечить оптимальную производительность системы, используйте SSL только для сеансов, где это необходимо. Добавьте на сервер IBM Spectrum Protect дополнительные ресурсы процессора, чтобы удовлетворить возросшие требования.

Linux: Форматирование базы данных и журнала

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.

После конфигурирования связей сервера все готово для инициализации базы данных. Проверьте, что вы вошли в систему под ID пользователя экземпляра. Каталоги не должны находиться в файловых системах, где может закончиться свободное пространство. Если какие-либо каталоги (например, каталог архивного журнала) окажется недоступен или переполнен, сервер остановится.

Как настроить обработчик списков завершения работы

Задайте для переменной реестра DB2NOEXITLIST значение ON для каждого экземпляра сервера. Войдите в систему от имени владельца экземпляра сервера и введите команду:

```
db2set -i имя_экземпляра_сервера
DB2NOEXITLIST=ON
```

Например:  Операционные системы Linux

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Инициализация экземпляра сервера

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. Например, если каталог экземпляра сервера - это */tsminst1*, введите следующие команды:  Операционные системы Linux

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Совет: Если вы зададите несколько каталогов, убедитесь, что размеры соответствующих файловых систем равны, что позволит обеспечить непротиворечивую степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.
 Операционные системы LinuxСовет: Если DB2 не запустится после ввода команды DSMSERV FORMAT, возможно, надо выключить опцию монтирования файловой системы NOSUID. Если эта опция задана для файловой системы, содержащей каталог владельца экземпляра DB2, или для файловой системы, где находится база данных DB2, активные, архивные и резервные журналы или зеркальные копии журналов, ее (опцию) нужно выключить, чтобы можно было запустить систему.
После отключения опции NOSUID повторите монтирование файловой системы и запустите DB2, введя следующую команду:

```
db2start
```

Информация, связанная с данной:
DSMSERV FORMAT (форматирование базы данных и журнала)

Linux: Подготовка менеджера базы данных к резервному копированию базы данных

Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Об этой задаче

 Операционные системы LinuxНачиная с IBM Spectrum Protect V7.1.1 больше нет необходимости задавать пароль API во время конфигурирования сервера вручную. Если задать пароль API в процессе конфигурирования вручную, то попытки резервного копирования базы данных могут завершиться неудачно.

Если вы создаете экземпляр сервера IBM Spectrum Protect при помощи мастера по конфигурированию, то вам не нужно выполнять эти действия. Если вы конфигурируете экземпляр вручную, выполните описанные ниже шаги, прежде чем вводить команду BACKUP DB или RESTORE DB.

Внимание: Если база данных недоступна, весь сервер IBM Spectrum Protect становится недоступным. Если база данных утеряна и ее нельзя восстановить, может оказаться затруднительным или даже невозможным восстановить данные,

которыми управляет этот сервер. Поэтому очень важно создать резервную копию базы данных.
Операционные системы LinuxВ следующих командах замените значения из примера фактическими значениями. В примерах используется значение `tsminst1` в качестве ID пользователя экземпляра сервера, /tsminst1 в качестве каталога экземпляра сервера и /home/tsminst1 в качестве домашнего каталога пользователя экземпляра сервера.

1. Задайте конфигурацию переменных среды API IBM Spectrum Protect для экземпляра базы данных:
   a. Войдите в систему от имени ID пользователя `tsminst1`.
   b. После входа пользователя `tsminst1` в систему убедитесь, что среда DB2 правильно инициализирована. Среда DB2 инициализируется путем запуска сценария /home/tsminst1/sqllib/db2profile, который обычно запускается автоматически из профиля ID пользователя. Убедитесь, что в домашнем каталоге пользователя экземпляра существует файл `.profile`, например, /home/tsminst1/.profile. Если `.profile` не запускает сценария `db2profile` добавьте в него следующие строки:

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; then
            . /home/tsminst1/sqllib/db2profile
        fi
      ```

   c. Добавьте в файл каталог_экземпляра/sqllib/userprofile следующие строки:

      ```
      DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
      DSMI_DIR=каталог_bin_сервера/dbbkapi
      DSMI_LOG=каталог_экземпляра_сервера
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      Здесь используются следующие обозначения:
      - *каталог_экземпляра* - это домашний каталог пользователя экземпляра сервера.
      - *каталог_экземпляра_сервера* - это каталог экземпляра сервера.
      - *каталог_сервера_bin* - это каталог bin сервера. Каталог по умолчанию - /opt/tivoli/tsm/server/bin.

      Добавьте в файл каталог_экземпляра/sqllib/usercshrc следующие строки:

      ```
      setenv DSMI_CONFIG=каталог_экземпляра_сервера/tsmdbmgr.opt
      setenv DSMI_DIR=каталог_bin_сервера/dbbkapi
      setenv DSMI_LOG=каталог_экземпляра_сервера
      ```

2. Выйдите из системы и снова войдите в нее от имени `tsminst1` либо введите команду:

   ```
   . ~/.profile
   ```

   Совет: Убедитесь, что после начальной точки (.) введен пробел.
3. Создайте файл с именем `tsmdbmgr.opt` в каталоге *экземпляр_сервера*, который в этом примере находится в каталоге /tsminst1, и добавьте в него следующую строку:

   ```
   SERVERNAME TSMDBMGR_TSMINST1
   ```

   Напоминание: Значение `SERVERNAME` должно совпадать в файлах `tsmdbmgr.opt` и `dsm.sys`.
4. От имени пользователя root добавьте в файл конфигурации API IBM Spectrum Protect `dsm.sys` указанные ниже строки. По умолчанию файл конфигурации `dsm.sys` находится в следующем каталоге:
   - *каталог_сервера_bin*/dbbkapi/dsm.sys

   ```
   servername TSMDBMGR_TSMINST1
   commmethod         tcpip
   tcpserveraddr localhost
   tcpport            1500
   errorlogname /tsminst1/tsmdbmgr.log
   nodename $$_TSMDBMGR_$$
   ```

   где
   - *servername* соответствует значению `servername` в файле `tsmdbmgr.opt`.
   - *commethod* задает API клиента, используемый для связи с сервером при резервном копировании базы данных. Это может быть значение `tcpip` или `sharedmem`. Дополнительную информацию о совместно используемой памяти смотрите в описании шага 5.
   - *tcpserveraddr* задает адрес сервера, который API клиента будет использовать для связи с сервером для резервного копирования базы данных. Для резервного копирования базы данных надо задать значение `localhost`.
   - *tcpport* задает номер порта, который API клиента будет использовать для связи с сервером с целью резервного копирования базы данных. Значение `tcpport` должно быть значением, которое задано в файле опций сервера dsmserv.opt.

- *errorlogname* задает журнал ошибок, в который API клиента будет записывать ошибки, происходящие при резервном копировании базы данных. Обычно этот журнал находится в каталоге экземпляра сервера. Однако его можно поместить в любой другой каталог, разрешения на запись в который есть у ID пользователя.
- *nodename* задает имя узла, которое API клиента будет использовать для соединения с сервером при резервном копировании базы данных. Чтобы обеспечить возможность резервного копирования базы данных, нужно задать значение `$$_TSMDBMGR_$$`.

 Операционные системы LinuxВнимание: Не добавляйте в опцию PASSWORDACCESS generate в файл конфигурации dsm.sys. Эта опция может привести к сбою резервного копирования базы данных.

5. Необязательно: Сконфигурируйте сервер для резервного копирования базы данных с использованием совместно используемой памяти. Таким образом вы можете уменьшить нагрузку на процессор и увеличить пропускную способность. Сделайте следующее:
   a. Просмотрите файл dsmserv.opt. Если следующие строки отсутствуют в этом файле, то добавьте их:

      ```
      commmethod     sharedmem
      shmport номер_порта
      ```

      где *номер_порта* задает порт, используемый для совместно используемой памяти.
   b. В файле конфигурации dsm.sys найдите следующие строки:

      ```
      commmethod        tcpip
      tcpserveraddr localhost
      tcpport номер_порта
      ```

      Замените указанные строки следующими строками:

      ```
      commmethod     sharedmem
      shmport номер_порта
      ```

      где *номер_порта* задает порт, используемый для совместно используемой памяти.

Linux: Опции конфигурирования сервера для обслуживания сервера баз данных

Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

Об этой задаче

Для реорганизации таблиц и индексов требуются значительные процессорные ресурсы, пространство для активного журнала и пространство для архивного журнала. Поскольку резервное копирование баз данных имеет приоритет перед реорганизацией, выберите время и длительность для реорганизации так, чтобы эти процессы не перекрывались и реорганизация смогла завершиться.

 Операционные системы LinuxВы можете оптимизировать реорганизацию индекса и таблиц для базы данных сервера. Таким образом можно избежать неожиданного роста базы данных и проблем, отрицательно влияющих на производительность. Инструкции смотрите в техническом примечании 1683633.

Если вы изменяете эти опции сервера при работающем сервере, надо остановить и перезапустить сервер, чтобы они вступили в силу.

Процедура

1. Измените опции сервера.
    Операционные системы LinuxОтредактируйте файл опций сервера dsmserv.opt в каталоге экземпляра сервера. При изменении файла опций сервера придерживайтесь следующих рекомендаций:
   - Чтобы включить опцию, удалите звездочку в начале строки.
   - Введите опцию в любой строке.
   - Вводите по одной опции на строке. Вся опция со своим значением должна быть записана на одной строке.
   - Если для одной опции в файле есть несколько записей, сервер использует последнюю запись.

Чтобы просмотреть доступные опции сервера, воспользуйтесь файлом примера dsmserv.opt.smp в каталоге /opt/tivoli/tsm/server/bin.

2. Если вы собираетесь использовать дедупликацию данных, то разрешите опцию сервера ALLOWREORGINDEX. Добавьте следующую опцию и значение в файл опций сервера:

   ```
   allowreorgindex yes
   ```

3. Задайте опции сервера REORGBEGINTIME и REORGDURATION, управляющие моментом начала реорганизации и ее длительностью. Выберите время и длительность, чтобы выполнять реорганизацию во время ожидаемой минимальной занятости сервера. Эти опции сервера действуют на процессы реорганизации как таблиц, так и индексов.
   a. Задайте время начала реорганизации при помощи опции сервера REORGBEGINTIME. Задайте время по 24-часовой системе. Например, чтобы начать реорганизацию в 8.30 вечера, задайте в файле опций сервера:

      ```
      reorgbegintime 20:30
      ```

   b. Задайте интервал, в который сервер может начать реорганизацию. Например, чтобы указать, что сервер может начать реорганизацию в течении четырех часов после времени, заданного опцией сервера REORGBEGINTIME, задайте в файле опций сервера:

      ```
      reorgduration 4
      ```

4. Если в момент изменения файла опций сервера сервер работает, остановите и перезапустите его.

Операционные системы Linux

Linux: Запуск экземпляра сервера

Сервер можно запускать от имени ID пользователя экземпляра (что является предпочтительным методом) или от имени ID пользователя root.

Прежде чем начать

Убедитесь, что вы правильно задали разрешения и пределы пользователя.

Операционные системы LinuxИнструкции смотрите в разделе Проверка прав доступа и ограничений для пользователей.

Об этой задаче

При запуске сервера с использованием ID пользователя экземпляра упрощается процесс конфигурирования и исключаются потенциальные проблемы. Однако в некоторых случаях может потребоваться запуск сервера под ID пользователя root. Например, вы можете захотите использовать ID пользователя root, чтобы сервер мог обращаться к определенным устройствам. Можно настроить автоматический запуск сервера, используя либо ID пользователя экземпляра, либо ID пользователя root.

Операционные системы LinuxЕсли вам нужно выполнить задачи по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания.

Процедура

Чтобы запустить сервер, выполните одно из следующих действий:

- Запустите сервер от имени ID пользователя экземпляра.

  Операционные системы LinuxИнструкции смотрите в разделе Запуск сервера от имени ID пользователя экземпляра.

- Запустите сервер от имени ID пользователя root.

  Инструкции по авторизации ID пользователей root для запуска сервера смотрите на веб-странице Авторизация ID пользователей root для запуска сервера (V7.1.1). Инструкции по запуску сервера с ID пользователя root смотрите на веб-странице Запуск сервера от имени ID пользователя root (V7.1.1).

- Операционные системы LinuxАвтоматический запуск сервера.

Операционные системы LinuxИнструкции смотрите в разделе Linux: Автоматический запуск серверов в системах Linux.

- Операционные системы LinuxЗапустите сервер в режиме обслуживания.

  Инструкции смотрите в разделе Linux: Запуск сервера в режиме обслуживания.

Операционные системы Linux

Linux: Проверка прав доступа и ограничений для пользователей

Перед запуском сервера проверьте права доступа и пределы пользователя.

Об этой задаче

Если не проверить пользовательские пределы (другое название - *значения ulimit*, могут возникнуть нестабильность или ошибки ответов сервера. Нужно также проверить предел для максимального числа открытых файлов, установленный на уровне системы. Этот предел на уровне системы не может быть меньше пользовательского предела.

Процедура

1. Убедитесь, что у ID пользователя экземпляра сервера есть разрешения на запуск сервера.
2. Для экземпляра сервера, который вы собираетесь запускать, убедитесь, что у вас есть полномочия на чтение и запись файлов в каталоге этого экземпляра сервера. Проверьте, что в каталоге экземпляра сервера существует файл dsmserv.opt и он включает в себя параметры для экземпляра сервера.
3. Если сервер подключается к ленточному накопителю, чейнджеру носителей или устройству со сменными носителями, а вы собираетесь запускать сервер под ID пользователя экземпляра сервера, предоставьте этому ID пользователя доступ на чтение и запись для указанных устройств. Чтобы задать разрешения, выполните одно из следующих действий:
   - Если система выделена для IBM Spectrum Protect и доступ есть только у администратора IBM Spectrum Protect, задайте для специального файла устройства общий доступ с правом записи. Введите в командной строке операционной системы следующую команду:

     ```
     chmod +w /dev/rmtX
     ```

   - Если в системе несколько пользователей, вы можете ограничить доступ, сделав ID пользователя экземпляра IBM Spectrum Protect владельцем специальных файлов устройств. Введите в командной строке операционной системы следующую команду:

     ```
     chmod u+w /dev/rmtX
     ```

   - Если на одном и том же компьютере работают экземпляры нескольких пользователей, измените имя группы, например, TAPEUSERS, и добавьте в эту группу каждый ID пользователя экземпляра IBM Spectrum Protect. Затем измените для специальных файлов устройств владельца, так чтобы их владельцем стала группа TAPEUSERS, и предоставьте группе разрешение на запись этих файлов. Введите в командной строке операционной системы следующую команду:

     ```
     chmod g+w /dev/rmtX
     ```

4. Операционные системы Linux Если используется драйвер устройств IBM Spectrum Protect и утилита autoconf, предоставьте при помощи опции -a доступ с правом чтения/записи этому ID пользователя экземпляра.
5. Операционные системы LinuxЧтобы предотвратить отказы сервера при взаимодействии с DB2, настройте параметры ядра.

   Операционные системы LinuxИнструкции о настройке параметров ядра смотрите в разделе Linux: Настройка параметров ядра для систем Linux.

6. Проверьте следующие пределы пользователя на соответствие рекомендациям в таблице.

Табл. 1. Значения пользовательского предела (ulimit)

Тип пользовательского предела	Рекомендуемое значение	Команда для запроса значения
Максимальный размер создаваемых файлов ядра	Без ограничений	`ulimit -Hc`

Тип пользовательского предела	Рекомендуемое значение	Команда для запроса значения
Максимальный размер сегмента данных для процесса	Без ограничений	`ulimit -Hd`
Максимальный размер файлов	Без ограничений	`ulimit -Hf`
Максимальное число открытых файлов	65536	`ulimit -Hn`
Максимальное время процессора в секундах	Без ограничений	`ulimit -Ht`

Чтобы изменить пользовательские пределы, выполните инструкции в документации к используемой операционной системе.

Совет: Если вы собираетесь запускать сервер автоматически при помощи сценария, пользовательские пределы можно задать в этом сценарии.

7. Убедитесь, что для пользовательского предела максимального числа пользовательских процессов (`параметр nproc`) задано минимальное рекомендуемое значение 16384.
   a. Для проверки текущего пользовательского значения введите команду`ulimit -Hu` от имени ID пользователя экземпляра. Например:

   ```
   [user@Machine ~]$ ulimit -Hu
   16384
   ```

   b. Если предел максимального числа пользовательских процессов не равен 16384, то задайте значение 16384.
   Операционные системы LinuxДобавьте следующую строку в файл /etc/security/limits.conf:

   ```
   ID_пользователя_экземпляра        -    nproc          16384
   ```

   где *ID_пользователя_экземпляра* - это ID пользователя экземпляра сервера.
   Операционные системы LinuxЕсли сервер установлен в операционной системе Red Hat Enterprise Linux 6, задайте пользовательский предел, отредактировав файл /etc/security/limits.d/90-nproc.conf в каталоге /etc/security/limits.d. Этот файл перезаписывает значения в файле /etc/security/limits.conf.
   Совет: Предельное значение по умолчанию для максимального числа пользовательских процессов изменено в некоторых дистрибутивах и версиях операционной системы Linux. Значение по умолчанию - 1024. Если не изменить это значение на минимальное предлагаемое значение 16384, возможны отказы и зависания сервера.

Операционные системы Linux

Linux: Запуск сервера от имени ID пользователя экземпляра

Чтобы запустить сервер под ID пользователя экземпляра, войдите в систему с ID пользователя root и введите в каталоге экземпляра сервера соответствующую команду.

Прежде чем начать

Убедитесь, что права доступа и пределы пользователей заданы правильно. Инструкции смотрите в разделе Linux: Проверка прав доступа и ограничений для пользователей.

Процедура

1. Войдите в систему, в которой установлен IBM Spectrum Protect, от имени ID пользователя экземпляра для сервера.
2. Если у вас нет профиля пользователя, который запускает сценарий `db2profile`, то введите следующую команду:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Совет: Инструкции об изменении сценария входа в систему ID пользователя для автоматического запуска сценария `db2profile` смотрите в документации по DB2.
3. Запустите сервер, введя следующую команду в одной строке из каталога экземпляра сервера:

   Операционные системы Linux

   ```
   usr/bin/dsmserv
   ```

Совет: Эта команда выполняется в режиме активного окна, так что вы сможете задать ID администратора и соединиться с экземпляром сервера.
 Операционные системы LinuxНапример, если имя экземпляра сервера - `tsminst1`, а каталог экземпляра сервера - /tsminst1, введите следующие команды:

```
cd /tsminst1
 . ~/sqllib/db2profile
/usr/bin/dsmserv
```

 Операционные системы Linux

Linux: Автоматический запуск серверов в системах Linux

Используйте для автоматического запуска сервера в Linux сценарий dsmserv.rc.

Прежде чем начать

Убедитесь, что правильно заданы параметры ядра. Инструкции смотрите в разделе Настройка параметров ядра для систем Linux.

Убедитесь в том, что экземпляр сервера запущен от имени ID пользователя владельца экземпляра.

Убедитесь в том, что правильно заданы права доступа и пользовательские пределы. Инструкции смотрите в разделе Проверка прав доступа и пределов пользователя.

Об этой задаче

Сценарий dsmserv.rc расположен в каталоге установки сервера, например, /opt/tivoli/tsm/server/bin.

Сценарий dsmserv.rc можно использовать для запуска сервера вручную или же автоматически, если добавить записи в каталог /etc/rc.d/init.d. Этот сценарий работает с утилитами Linux, такими как CHKCONFIG и SERVICE.

Процедура

Для каждого экземпляра сервера, который вы хотите запускать автоматически, выполните следующие действия:

1. Поместите копию сценария dsmserv.rc в каталог /init.d, например, в /etc/rc.d/init.d.

   Убедитесь, что вы изменяете только копию сценария. Не изменяйте исходный сценарий.

2. Переименуйте копию сценария, чтобы она соответствовала владельцу экземпляра сервера, например: `tsminst1`.

   В созданном сценарии предполагается, что каталог экземпляра сервера - *домашний_каталог*/tsminst1, например: /home/tsminst1/tsminst1.

3. Если каталог экземпляра сервере - не *домашний_каталог*/tsminst1, найдите в копии сценария следующую строку:

   ```
   instance_dir="${instance_home}/tsminst1"
   ```

   Измените эту строку так, чтобы она указывала на используемый каталог экземпляра сервера, например:

   ```
   instance_dir="/tsminst1"
   ```

4. Найдите в копии сценария следующую строку:

   ```
   # pidfile: /var/run/dsmserv_instancename.pid
   ```

   Замените имя экземпляра на имя владельца экземпляра сервера. Например, если имя владельца экземпляра tsminst1, то измените строку так:

   ```
   # pidfile: /var/run/dsmserv_tsminst1.pid
   ```

5. Сконфигурируйте уровень выполнения, на котором должен автоматически запускаться сервер. При помощи таких инструментов, как утилита CHKCONFIG, задайте значение, соответствующее многопользовательскому режиму с включенной поддержкой работы по сети. Как правило, используется уровень выполнения 3 или 5, в зависимости от операционной системы и ее конфигурации. Дополнительную информацию о многопользовательском режиме и уровнях выполнения смотрите в документации для используемой операционной системы.

6. Чтобы запустить или остановить сервер, введите одну из следующих команд:
   - Чтобы запустить сервер:

     ```
     service tsminst1 start
     ```

   - Чтобы остановить сервер:

     ```
     service tsminst1 stop
     ```

Пример

В этом примере используются следующие значения:

- Владелец экземпляра - tsminst1.
- Каталог экземпляра сервера - /home/tsminst1/tsminst1.
- Имя копии сценария dsmserv.rc - `tsminst1`.
- Для конфигурирования запуска сценария с уровнями выполнения 3, 4 и 5 используется утилита CHKCONFIG.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_instancename.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Информация, связанная с данной:
Сценарий запуска сервера: dsmserv.rc
Операционные системы Linux

Linux: Запуск сервера в режиме обслуживания

Сервер можно запустить в режиме обслуживания, чтобы избежать повреждений при выполнении задач по обслуживанию и переконфигурированию.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

   ```
   halt
   ```

2. Запустите сервер, используя метод, который вы используете в производственном режиме.

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Linux: Остановка сервера

При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.

Об этой задаче

Чтобы остановить сервер, введите в командной строке IBM Spectrum Protect следующую команду:

```
halt
```

 Операционные системы LinuxЕсли невозможно подключиться к серверу в качестве клиента администрирования, но нужно остановить сервер, следует отменить процесс с помощью команды kill с указанием идентификационного номера (pid) процесса. Значение pid будет показано при инициализации.
Важное замечание: Перед тем, как ввести команду kill, убедитесь что вам известен правильный идентификатор сервера IBM Spectrum Protect.
Для определения номера процесса, который нужно выгрузить, можно использовать файл `dsmserv.v6lock` в том каталоге, из которого запущен сервер. Чтобы увидеть файл, введите:

```
cat /instance_dir/dsmserv.v6lock
```

 Операционные системы LinuxЧтобы остановить сервер, введите следующую команду:

```
kill -23 dsmserv_pid
```

где *dsmserv_pid* - это числовой ID процесса.

Linux: Регистрация лицензий

Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.

Об этой задаче

Используйте для этого команду REGISTER LICENSE. Дополнительные сведения смотрите в разделе REGISTER LICENSE.

Пример: Зарегистрировать лицензию

Зарегистрируйте базовую лицензию на IBM Spectrum Protect.

```
register license file=tsmbasic.lic
```

Linux: Подготовка сервера к операциям резервного копирования базы данных

Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.

Процедура

1. Убедитесь, что конфигурация IBM Spectrum Protect - полная. Если вы не используете мастер конфигурирования (dsmicfgx) для конфигурирования сервера, убедитесь, что вы выполнили шаги по конфигурированию сервера вручную для резервного копирования базы данных.
2. Выберите класс устройств, который следует использовать для резервного копирования базы данных, защитите главный ключ шифрования и задайте пароль. Все эти действия выполняются путем ввода команды SET DBRECOVERY из административной командной строки:

   ```
   set dbrecovery имя_класса_устройств protectkeys=yes password=имя_пароля
   ```

   где *имя_класса_устройств* задает класс устройств, который следует использовать для операций резервного копирования базы данных, а *имя_пароля* задает пароль.
   Вы обязательно должны задать имя класса устройств, иначе резервное копирование завершится неудачно. Задав PROTECTKEYS=YES, вы сделаете так, что во время операций резервного копирования базы данных будет создаваться резервная копия главного ключа шифрования.
   Важное замечание: Создайте надежный пароль, содержащий хотя бы 8 символов. Убедитесь, что вы запомнили этот пароль. Если задан пароль для резервной копии базы данных, вы должны указать тот же самый пароль в команде RESTORE DB для восстановления базы данных.

Пример

Чтобы указать, что резервные копии базы данных содержат копию главного ключа шифрования для сервера, введите следующую команду:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Linux: Запуск нескольких экземпляров серверов на одном компьютере

Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.

Умножьте требования к памяти и другим системным ресурсам для одного сервера на число экземпляров, которые вы собираетесь создать в системе.

 Операционные системы LinuxНабор файлов для одного экземпляра сервера хранится отдельно от файлов, используемым другим экземпляром сервера в той же системе. Выполните для каждого нового экземпляра шаги, описанные в разделе Linux: Создание экземпляра сервера, включая создание пользователя нового экземпляра.

Чтобы управлять объемом системной памяти, используемым каждым сервером, задайте опцию DBMEMPERCENT, позволяющую ограничить процент системной памяти. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.

Можно произвести обновление V7.1 до V8.1 напрямую. Более подробную информацию смотрите в разделе об обновлении (Обновление до V8.1). Если при обновлении в вашей системе есть несколько серверов, запускать мастер установки нужно только один раз. Мастер установки соберет информацию о базах данных и переменных для всех исходных экземпляров сервера.

Если вы выполняете обновление IBM Spectrum Protect V6.3 до V8.1.5 и в системе есть несколько серверов, то все экземпляры, существующие в DB2 V9.7, удаляются и заново создаются в DB2 V11.1. Мастер сгенерирует команду `db2 upgrade db имя_бд` для каждой базы данных. В процессе обновления также будет произведено переконфигурирование переменных среды базы данных для каждого экземпляра в вашей системе.

Задачи, связанные с данной:
Запуск нескольких экземпляров серверов на одном компьютере (V7.1.1)

Linux: Мониторинг сервера

Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Процедура

1. Следите за активным журналом, чтобы убедиться, что его размер соответствует рабочей нагрузке, обрабатываемой экземпляром сервера.

   Если уровень рабочей нагрузки на сервер приближается к типичному ожидаемому уровню, то объем пространства, используемого активным журналом, составляет 80-90% пространства. В этот момент, возможно, нужно увеличить объем пространства. Необходимость увеличения пространства зависит от типов транзакций, составляющих рабочую нагрузку сервера. Характеристики транзакций влияют на то, как используется пространство активного журнала.

   На использованием пространства активного журнала могут влиять следующие характеристики транзакций:

   - Число и размер файлов в операциях резервного копирования.
     - Такие клиенты, как файл-серверы, которые создают резервные копии большого числа мелких файлов, могут инициировать большое число быстро завершающихся транзакций. Транзакции могут использовать большой объем пространства в активном журнале, но кратковременно.
     - Такие клиенты, как почтовый сервер или сервер базы данных, которые создают резервные копии больших объемов данных в ходе немногочисленных транзакций, могут инициировать небольшое число транзакций, для завершения которых требуется длительное время. Транзакции могут использовать небольшой объем пространства в активном журнале, но в течение длительного времени.
   - Типы соединений с сетью
     - Транзакции, связанные с операциями резервного копирования, которые выполняются с использованием высокоскоростных сетевых соединений, завершаются быстрее. Транзакции используют пространство в активном журнале в течение более короткого времени.
     - Для завершения транзакций, связанных с операциями резервного копирования, которые выполняются с использованием относительно низкоскоростных сетевых соединений, требуется больше времени. Транзакции используют пространство в активном журнале в течение более длительного времени.

   Если сервер обрабатывает транзакции с широким диапазоном характеристик, то пространство, используемое для активного журнала, может значительно увеличиваться и уменьшаться с течением времени. В этом случае вы должны сделать так, чтобы, как правило, использовался меньший процент пространства активного журнала. Дополнительное пространство позволит активному журналу увеличиваться в размере, если для выполнения транзакций требуется очень много времени.

2. Следите за архивным журналом, чтобы убедиться в том, что для него всегда хватает места.
   Напоминание: Если архивный журнал и архивный журнал отказоустойчивости заполнятся, может заполниться активный журнал, и сервер остановится. Цель заключается в том, чтобы архивному журналу был доступен достаточный объем пространства и он никогда не использовал все доступное ему пространство.
   Вы, вероятно, заметите следующие закономерности:
   a. Сначала архивный журнал быстро растет по мере выполнения операций резервного копирования клиента.
   b. Резервное копирование базы данных производится регулярно либо по расписанию, либо вручную.
   c. После выполнения, как минимум, двух операций полного резервного копирования базы данных сокращение журналов происходит автоматически. В результате отбрасывания пространство, используемое архивным журналом, уменьшается.
   d. Обычные операции клиента продолжаются, и архивный журнал снова растет.
   e. Резервное копирование базы данных выполняется регулярно, и отбрасывание журналов происходит так же часто, как и операции полного резервного копирования базы данных.

   При таких закономерностях архивный журнал сначала растет, затем уменьшается, а затем может снова вырасти. С течением времени, по мере продолжения нормальной работы, объем пространства, используемого архивным журналом, должен достичь относительно постоянного уровня.

   Если архивный журнал продолжает расти, то выполните одно из описанных ниже действий или оба эти действия:
   - Добавьте пространство для архивного журнала. Это может означать перемещение архивного журнала в другую файловую систему.
   - Увеличьте частоту полного резервного копирования базы данных, чтобы отбрасывание журналов производилось чаще.
3. Если вы задали каталог для резервного архивного журнала, определите, сохраняются ли в этом каталоге какие-либо журналы при обычной работе. Если пространство резервного журнала используется, то увеличьте размер архивного журнала. Цель состоит в том, чтобы резервный архивный журнал использовался только в экстраординарных условиях, а не при обычной работе.

Linux: Установка пакета исправлений сервера IBM Spectrum Protect

Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.

Прежде чем начать

Чтобы установить на сервер пакет Fix Pack или промежуточный пакет исправлений, установите сервер требуемого для выполнения уровня. Не обязательно запускать установку сервера на уровне базового выпуска. Например, если у вас установлена версия 8.1.1, то можно перейти сразу к самому последнему пакету Fix Pack для V8.1. Не обязательно начинать с установки V8.1.0, если доступно текущее изменение.

У вас должен быть установлен пакет лицензий IBM Spectrum Protect. Пакет лицензий приобретается вместе с базовым выпуском программного обеспечения. При загрузке пакета исправлений или промежуточного пакета исправлений с сайта Fix Central установите лицензию на сервер, которая есть на веб-сайте Passport Advantage. Для вывода сообщений и справки на языке, ином чем американский английский, установите языковый пакет по своему выбору.

Если вы обновляете сервер до V8.1.5 или новее, а затем возвращаетесь к уровню сервера, более раннему, чем V8.1.5, необходимо восстановить базу данных на момент времени, предшествующий обновлению. Во время процесса обновления выполните требуемые действия, обеспечивающие возможность восстановления базы данных: создайте резервные копии базы данных, файла хронологии тома, файла конфигурации устройств и файла опций сервера. Дополнительные сведения смотрите в разделе Linux: Возврат от версии 8.1.5 к предыдущему серверу.

Если вы используете службу управления клиентами, убедитесь, что вы обновили ее до той же версии, к которой относится сервер IBM Spectrum Protect.

Убедитесь, что вы сохранили установочный носитель базового выпуска установленного сервера. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.

Посетите страницу Портал поддержки IBM® и найдите там следующую информацию:

- Список последних исправлений и их скачивание. Щелкните по **Downloads** (Материалы для скачивания) и примените все соответствующие исправления.
- Подробности получения базового пакета лицензий. Найдите **Downloads > Passport Advantage** (Материалы для скачивания - Passport Advantage).
- Поддерживаемые платформы и системные требования. Укажите для поиска: **поддерживаемые операционные системы IBM Spectrum Protect**.

Обязательно обновите сервер, прежде чем обновлять клиенты резервного копирования и архивирования. Если не обновить сначала сервер, связь между серевром и клиентами может прерваться.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

Процедура

Чтобы установить пакет исправлений или промежуточное исправление, сделайте следующее:

1. Создайте резервную копию базы данных. Рекомендуется способ использовать резервное копирование в режиме снимка. Резервное копирование в режима снимка - это полное резервное копирование базы данных, не прерывающее никаких плановых операций резервного копирования базы данных. Например, введите следующую команду управления IBM Spectrum Protect:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте резервную копию информации о конфигурации устройств. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup devconfig filenames=имя_файла
   ```

где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.

3. Сохраните файл хронологии томов в другом положении или переименуйте этот файл. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt. Этот файл расположен в каталоге экземпляра сервера.
5. Прежде чем устанавливать пакет исправлений или промежуточное исправление, остановите сервер. Используйте команду HALT.
6. Убедитесь, что в каталоге установки доступно дополнительное пространство. Установка этого пакета Fix Pack может потребовать дополнительного временного дискового пространства в каталоге установки сервера. Объем дополнительного дискового пространства может быть таким же, как требуется для установки новой базы данных как части установки IBM Spectrum Protect. Мастер по установке IBM Spectrum Protect показывает объем пространства, требуемого для установки пакета Fix Pack, и доступный объем пространства. Если требуемый объем пространства превышает доступный, установка прекращается. Если установка остановилась, добавьте требуемое дисковое пространство к файловой системе и перезапустите установку.
7. Операционные системы LinuxВойдите в систему от имени пользователя root.
8. Получите файл пакета исправлений или промежуточного исправления, который вы хотите установить, со страниц Портал поддержки IBM, Passport Advantage или Fix Central.
9. Операционные системы LinuxПерейдите в каталог, куда вы поместили выполняемый файл, и сделайте следующее.
   Совет: Файлы извлекаются в текущий каталог. Убедитесь, что исполняемый файл находится в каталоге, куда будут извлекаться файлы.
   a. Измените разрешения на доступ к файлам, введя следующую команду:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-платформа.bin
      ```

      где *платформа* - это архитектура, в которой устанавливается IBM Spectrum Protect.
   b. Чтобы извлечь файлы установки, введите следующую команду:

      ```
      ./8.x.x.x-IBM-SPSRV-платформа.bin
      ```

10. Выберите один из следующих способов установки IBM Spectrum Protect.
    Важное замечание: После установки пакета исправлений не нужно снова выполнять все шаги по конфигурированию. Вы можете остановить программу после завершения установки, исправить все ошибки и перезапустить свои серверы.
    Установите программное обеспечение IBM Spectrum Protect одним из следующих способов:

    Мастер установки
    : Выполните инструкции для вашей операционной системы.
      Linux: Установка IBM Spectrum Protect при помощи мастера установки

    Совет: Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.

    Командная строка в режиме консоли
    : Выполните инструкции для вашей операционной системы.
      Linux: Установка IBM Spectrum Protect в режиме консоли

    Режим без вывода сообщений
    : Выполните инструкции для вашей операционной системы.
      Linux: Установка IBM Spectrum Protect в режиме без вывода сообщений

    Совет: Если в вашей системе используется несколько экземпляров сервера, запустите мастер установки только один раз. Мастер по установке обновит все экземпляры сервера.

Результаты

Исправьте ошибки, обнаруженные в процессе установки.

Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по Файл > Просмотреть журнал. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по Справка > Экспорт данных для анализа ошибок.

Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:

- Операционные системы Linux/var/ibm/InstallationManager/logs

Linux: Возврат от версии 8.1.5 к предыдущему серверу

Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.

Прежде чем начать

У вас должны быть следующие элементы для более ранней версии сервера:

- Резервная копия базы данных сервера
- Файл хронологии тома
- Файл конфигурации устройств
- Файл серверных опций

Об этой задаче

Используйте одни и те же инструкции и для возврата к прежней версии в пределах одного выпуска (например, от 8.1.3 до 8.1.2 или от 8.1.3 до 7.1.2). Прежняя версия должна совпадать с версией, использовавшейся перед обновлением до версии 8.1.

Внимание: Задайте значение параметра REUSEDELAY, помогающее предотвратить потерю данных клиента резервного копирования и архивирования при возврате сервера к прежней версии.

Шаги по возврату к предыдущей версии сервера

Об этой задаче

Выполните следующие действия в системе, где установлен сервер версии 8.1:

Процедура

1. Остановите сервер, чтобы закрыть все операции сервера, с помощью команды HALT.
2. Удалите базу данных из менеджера базы данных, затем удалите каталоги базы данных и журналов восстановления.
   a. Вручную удалите базу данных. Один из способов удалить ее - ввести следующую команду:
   Операционные системы Linux

   ```
   dsmserv removedb tsmdb1
   ```

   b. Если вам нужно снова использовать пространство, занятое каталогами базы данных и журналов восстановления, вы теперь можете удалить эти каталоги.
3. Деинсталлируйте сервер V8.1 при помощи программы деинсталляции. При деинсталляции удаляется сервер и менеджер баз данных вместе с их каталогами. Дополнительные сведения смотрите в разделе Linux: Деинсталляция IBM Spectrum Protect.
4. Остановите службу кластеров. Заново установите версию программы сервера, которую вы использовали перед обновлением до V8.1.5. Эта версия должна совпадать с версией вашего сервера на момент создания резервной копии базы данных, которую вы восстановите в одном из последующих шагов. Например, перед обновлением сервер относился к версии 7.1.7, а вы собираетесь применить резервную копию базы данных, использовавшуюся на этом сервере. Чтобы получить возможность восстанавливать эту резервную копию базы данных, нужно установить Fix Pack для V7.1.7.
5. Сконфигурируйте новую базу данных сервера при помощи мастера конфигурирования. Чтобы запустить мастер, введите следующую команду: Операционные системы Linux

   ```
   . /dsmicfgx
   ```

6. Убедитесь, что нет серверов, запущенных в фоновом режиме.
7. Восстановите базу данных на заданный момент времени перед обновлением.

8. Скопируйте следующие файлы в каталог экземпляра.
    - Файл конфигурации устройств
    - Файл хронологии тома
    - Файл опций сервера (обычно, dsmserv.opt)
9. Если вы включили дедупликацию данных для каких-либо пулов хранения типа FILE, которые существовали перед обновлением, или если вы при использовании сервера V8.1.5 перенесли данные, существовавшие перед обновлением, в новые пулы хранения, вы должны будете выполнить дополнительные шаги по восстановлению. Дополнительные сведения смотрите в разделе Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных.
10. Если значение параметра REUSEDELAY для пулов хранения меньше возраста восстанавливаемой вами базы данных, восстановите тома во всех пулах хранения с последовательным доступом, которые были консолидированы после резервного копирования базы данных. Используйте команду RESTORE VOLUME.
    Если у вас нет резервной копии пула хранения, произведите аудит консолидированных томов при помощи команды AUDIT VOLUME с параметром FIX=YES для устранения противоречий. Например:

    ```
    audit volume имя_тома fix=yes
    ```

11. Если с использованием сервера версии 8.1 выполнялись операции резервного копирования или архивирования клиента, выполните аудит томов пулов хранения, на которых были сохранены эти данные.

Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных

Если во время работы сервера в версии 8.1.5 вы создавали новые пулы хранения, включали дедупликацию данных для любых пулов хранения типа FILE или совершали оба этих действия, необходимо выполнить некоторые дополнительные шаги, чтобы вернуться к предыдущей версии сервера.

Прежде чем начать

Чтобы вы смогли выполнить эту задачу, у вас должна быть полная резервная копия пула хранения, созданная до обновления до версии 8.1.5.

Об этой задаче

Используйте приведенную ниже информацию, если какое-то время у вас работал сервер V8.1.5 и вы в это время выполняли любое из следующих действий (или оба эти действия):

- Вы включили функцию дедупликации данных для любых пулов хранения, которые существовали до обновления до программы версии 8.1.5. Дедупликация данных применима только к пулам хранения, в которых используется тип устройств FILE.
- После обновления вы создали новые первичные пулы хранения *и* перенесли в эти новые пулы хранения данные, хранившиеся в других пулах хранения.

Выполните описанные ниже шаги после восстановления сервера до V7.

Процедура

- Для каждого пула хранения, для которого вы включили функцию дедупликации данных, восстановите весь пул хранения при помощи команды RESTORE STGPOOL.
- Для пулов хранения, созданных после обновления, определите, какие действия вам следует предпринять. Данные, перенесенные из существующих пулов хранения V8 в новые пулы хранения, могут быть потеряны, так как на восстановленном сервере V8 этих новых пулов не будет. Возможный способ выхода из этой ситуации зависит от типа пула хранения:
    - Если данные были перенесены в новый пул хранения из пулов хранения типа DISK, относящихся к V8, пространство, которое занимали перенесенные данные, вероятнее всего, было уже использовано повторно. Поэтому вы должны будете восстановить исходные пулы хранения V8, используя резервные копии этого пула хранения, созданные перед обновлением до V8.1.5.

      Если в новый пул хранения *не* переносились никакие данные из пулов хранения типа DISK, относящихся к V8, то произведите аудит томов пула хранения в этих пулах хранения типа DISK.

    - Если данные были перенесены в новый пул хранения из пулов хранения с последовательным доступом, относящихся к V8, эти данные могут все еще существовать на томах пула хранения на восстановленном

сервере V8 и быть пригодны для использования. Эти данные, вероятнее всего, будут пригодны для использования, если для параметра REUSEDELAY для этого пула хранения было задано значение, не позволившее произвести в нем консолидацию пространства, когда сервер работал как сервер V8.1.5. Если какие-либо тома были подвергнуты консолидации, когда сервер работал как сервер Версии 8.1.5, эти тома нужно будет восстановить из резервных копий пула хранения, созданных перед обновлением до V8.1.5.

Linux: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect

Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.

Назначение

Иногда после использования мастеров по установке и конфигурированию IBM Spectrum Protect вам потребуется ввести команды DB2. Ограниченный набор команд DB2, которые вы можете использовать (в частности, по указанию службы поддержки), представлен в списке в Табл. 1. Это не исчерпывающий список, он представлен только в виде дополнительного материала. Не предполагается, что администратор IBM Spectrum Protect будет ежедневно или вообще регулярно использовать эти команды. Приведены примеры использования некоторых команд. Подробности выходной информации не представлены.

Полное объяснение описанных здесь команд и их синтаксиса смотрите в Информационном центре Информация о DB2.

Табл. 1. Команды DB2

Команда	**Описание**	**Пример**
db2icrt	Создает экземпляры DB2 в домашнем каталоге владельца экземпляра. Совет: Мастер по конфигурированию IBM Spectrum Protect создает экземпляр, используемый сервером и базой данных. После того, как сервер установлен и сконфигурирован с помощью мастера по конфигурированию, команда db2icrt обычно не используется. Операционные системы LinuxЭта утилита находится в каталоге DB2DIR/instance, где DB2DIR представляет собой положение установки текущей версии системы баз данных DB2.	Создайте экземпляр IBM Spectrum Protect вручную.Введите команду в одной строке: `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`имя_экземпляра имя_экземпляра`*
db2set	Выводит переменные DB2.	Вывести список переменных DB2: `db2set`
CATALOG DATABASE	Сохраняет информацию о положении базы данных в системном каталоге баз данных. База данных может находиться или на локальной рабочей станции, или на удаленном сервере разделов базы данных. Мастер по конфигурированию серверов учитывает все каталоги, которые нужны для использования базы данных сервера. После того, как сервер сконфигурирован и запущен, вручную запустите эту команду, только если что-то в среде изменяется или повреждено.	Каталогизируйте базу данных: `db2 catalog database tsmdb1`

Команда	Описание	Пример
CONNECT TO DATABASE	Соединяется с заданной базой данных для использования интерфейса командной строки (command-line interface, CLI).	Соединитесь с базой данных IBM Spectrum Protect в интерфейсе командной строки DB2: `db2 connect to tsmdb1`

GET DATABASE CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Показать информацию конфигурации для алиаса базы данных:
		`db2 get db cfg for tsmdb1`
		Получить информацию для проверки параметров конфигурации базы данных, режима журналов и техобслуживания.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Получить информацию конфигурации для менеджера баз данных: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Получает информацию о состоянии работоспособности для менеджера баз данных и его баз данных. Возвращаемая информация представляет снимок состояния работоспособности на момент ввода команды. IBM Spectrum Protect отслеживает состояние базы данных при помощи снимка работоспособности и других механизмов, представленных DB2. Может так случиться, что снимок работоспособности или другой инструмент документации DB2 свидетельствует о возможном состоянии оповещения некоторого элемента или ресурса базы данных. Это означает, что нужно принять меры для исправления ситуации. IBM Spectrum Protect отслеживает условия и отвечает соответствующим образом. Обрабатываются не все выявленные оповещения DB2.	Получить отчет об индикаторах отслеживания работоспособности DB2: `db2 get health snapshot for database on tsmdb1`

Команда	Описание	Пример

GRANT (Полномочия базы данных)	Предоставляет полномочия, применимые ко всей базе данных, в отличие от привилегий, применимых к конкретным объектам в базе данных.	Предоставить доступ для ID пользователя itmuser:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Изменяет статистику, относящуюся к характеристикам таблицы и связанных индексов, или статистические производные таблицы. Эти характеристики включают в себя количество записей, количество страниц и среднюю длину записи. Запустите эту утилиту, чтобы увидеть таблицу после ее изменения или реорганизации. Производная таблица должна быть включена для оптимизации, чтобы ее можно было использовать для оптимизации запросов. Включенная для оптимизации производная таблица называется статистической производной таблицей. Используйте оператор DB2 ALTER VIEW , чтобы включить производную таблицу для оптимизации. Запустите утилиту RUNSTATS, когда изменения в рассматриваемых таблицах существенно влияют на возвращаемые в производной таблице строки. Совет: Сервер конфигурирует DB2 для запуска при необходимости команды RUNSTATS.	Изменить статистику для одной таблицы. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SETSCHEMA	Изменяет значение специального регистра CURRENT SCHEMA, подготавливаясь к вводу команд SQL непосредственно через интерфейс командной строки DB2. Совет: Специальный регистр - это область хранения, определенная для процесса применения менеджером баз данных. Он используется для хранения информации, на которую могут ссылаться операторы SQL.	Задать схему для IBM Spectrum Protect: `db2 set schema tsmdb1`
STARTDATABASEMANAGER	Запускает фоновые процессы текущего экземпляра менеджера баз данных. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Запустить менеджер баз данных: `db2start`

Команда	Описание	Пример
STOP DATABASE MANAGER	Останавливает текущий экземпляр менеджера баз данных. Менеджер баз данных остается активным, пока он не остановлен явным образом. Эта команда не останавливает экземпляр менеджера баз данных, если какие-либо приложения соединены с базами данных. Если соединений с базой данных нет, но есть подключения экземпляра, эти подключения экземпляра первыми принудительно прерываются данной командой. Затем она останавливает менеджер баз данных. Перед остановкой менеджера баз данных эта команда деактивирует также все невыполненные обращения к базе данных. Для клиента эта команда недопустима. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Остановить менеджер баз данных: `db2 stop dbm`

Linux: Деинсталляция IBM Spectrum Protect

Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Прежде чем начать

Прежде чем деинсталлировать IBM Spectrum Protect, выполните следующие шаги:

- Выполните полное резервное копирование базы данных.
- Сохраните копию хронологии томов и файлов конфигурации устройств.
- Поместите полученные тома в надежное место.

Об этой задаче

IBM Spectrum Protect можно деинсталлировать любым из следующих способов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

- Linux: Деинсталляция IBM Spectrum Protect при помощи графического мастера
  IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.
- Linux: Деинсталляция IBM Spectrum Protect в режиме консоли
  Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.
- Linux: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений
  Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.
- Linux: Деинсталляция и переустановка IBM Spectrum Protect
  Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.
- Linux: Деинсталляция IBM Installation Manager
  Можно деинсталлировать IBM Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Дальнейшие действия

Информацию о том, какие шаги по установке нужно выполнить, чтобы переустановить компоненты IBM Spectrum Protect, смотрите в разделе Linux: Установка компонентов сервера.

Linux: Деинсталляция IBM Spectrum Protect при помощи графического мастера

IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.

Процедура

1. Запустите Installation Manager.
    Операционные системы LinuxВ каталоге, в котором установлен Installation Manager, перейдите в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду:

   ```
   ./IBMIM
   ```

2. Щелкните по Деинсталлировать.
3. Выберите Сервер IBM Spectrum Protect и щелкните по Далее.
4. Щелкните по Деинсталлировать.
5. Щелкните по Готово.

Linux: Деинсталляция IBM Spectrum Protect в режиме консоли

Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   -  Операционные системы Linuxeclipse/tools

   Например:

   -  Операционные системы Linux/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду:
   -  Операционные системы Linux`./imcl -c`
3. Для деинсталляции введите `5`.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите `N` (Next - Далее).
6. Выберите деинсталляцию пакета сервера IBM Spectrum Protect.
7. Введите `N` (Next - Далее).
8. Введите `U` (Uninstall - Деинсталляция).
9. Введите `F` (Finish - Готово).

Linux: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений

Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции компонентов сервера IBM Spectrum Protect в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, uninstall_response_sample.xml, в каталоге input в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Если вы хотите деинсталлировать все компоненты IBM Spectrum Protect, оставьте заданное значение `modify="false"` для каждого компонента в файле ответов. Если вы не хотите деинсталлировать компонент, задайте значение `modify="true"`.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы Linuxeclipse/tools

   Например:

   - Операционные системы Linux/opt/IBM/InstallationManager/eclipse/tools
2. В каталоге tools введите следующую команду, где *файл_ответов* - это полное имя файла ответов:
   Операционные системы Linux

   ```
   ./imcl -input файл_ответов -silent
   ```

   Пример команды:

   Операционные системы Linux

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Linux: Деинсталляция и переустановка IBM Spectrum Protect

Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.

Об этой задаче

Чтобы вручную деинсталлировать и переустановить IBM Spectrum Protect, выполните следующие шаги:

1. Операционные системы LinuxПрежде чем приступать к деинсталляции, создайте список текущих экземпляров сервера. Введите команду:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Введите для каждого экземпляра сервера следующую команду:
   Операционные системы Linux

   ```
   db2 attach to имя_экземпляра
   db2 get dbm cfg show detail
   db2 detach
   ```

   Запишите путь базы данных для каждого экземпляра.
3. Деинсталлируйте IBM Spectrum Protect. Смотрите раздел Linux: Деинсталляция IBM Spectrum Protect.
4. При деинсталляции любой поддерживаемой версии IBM Spectrum Protect, включая пакет исправлений, создается файл экземпляра. Файл экземпляра создается для того, чтобы помочь вам переустановить IBM Spectrum Protect. Проверьте этот файл и используйте эту информацию, когда вас попросят ввести идентификационные данные экземпляра при переустановке. При установке в режиме без вывода сообщений вы предоставляете эти идентификационные данные при помощи переменной `INSTANCE_CRED`.
   Положение файла экземпляра:
   - Операционные системы Linux/etc/tivoli/tsm/instanceList.obj
5. Переустановите IBM Spectrum Protect. Смотрите раздел Linux: Установка компонентов сервера.

   Если файл `instanceList.obj` не существует, вы должны заново создать экземпляры сервера, используя следующие шаги:

   a. Заново создайте экземпляры сервера. Смотрите раздел Linux: Создание экземпляра сервера.
      Совет: Мастер установки сконфигурирует экземпляры сервера, но вы должны убедиться, что они существуют. Если они не существуют, вы должны будете сконфигурировать их вручную.
   b. Каталогизируйте базу данных. Поочередно войдите в систему от имени пользователя экземпляра для каждого экземпляра сервера и введите следующие команды:
      Операционные системы Linux

```
db2 catalog database tsmdb1
db2 attach to имя_экземпляра
db2 update dbm cfg using dftdbpath каталог_экземпляра
db2 detach
```

c.  Операционные системы LinuxУбедитесь, что экземпляр сервера создан успешно.Введите команду:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

d. Убедитесь, что IBM Spectrum Protect распознает экземпляры сервера, вызвав спи сок ваших каталогов. Вы увидите ваш домашний каталог (если вы его не изменили). Если вы использовали мастер конфигурирования, ваш каталог экземпляра не появится. Введите команду:

```
db2 list database directory
```

Если вы увидите в списке TSMDB1, вы можете запустить сервер.

Linux: Деинсталляция IBM Installation Manager

Можно деинсталлировать IBM® Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Прежде чем начать

Перед удалением IBM Installation Manager, необходимо убедиться, что все пакеты, установленные IBM Installation Manager, удалены. Закройте IBM Installation Manager перед запуском деинсталляции.

 Операционные системы LinuxДля просмотра установленных пакетов введите следующую команду в командной строке:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Процедура

Чтобы деинсталлировать IBM Installation Manager, выполните следующие шаги:

 Операционные системы Linux

1. Откройте командную строку и перейдите в каталог /var/ibm/InstallationManager/uninstall.
2. Введите следующую команду:

```
./uninstall
```

Ограничение: Вы должны войти в систему от имени ID пользователя `root`.

Windows: Установка сервера

Установка сервера включает в себя планирование, установку и первоначальное конфигурирование.

- Windows: Планирование установки сервера
  Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.
- Windows: Установка компонентов сервера
  Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.
- Windows: Первые шаги после установки IBM Spectrum Protect
  После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.
- Windows: Установка пакета исправлений сервера IBM Spectrum Protect
  Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.
- Windows: Возврат от версии 8.1.5 к предыдущему серверу
  Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые

файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.
- Windows: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect
  Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.
- Windows: Деинсталляция IBM Spectrum Protect
  Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Windows: Планирование установки сервера

Установите программное обеспечение сервера на компьютере, который управляет устройствами хранения, а программное обеспечение клиента - на каждой рабочей станции, которая передает данные в управляемое сервером IBM Spectrum Protect пространство хранения.

- Windows: Что нужно знать в первую очередь
  Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.
- Windows: Планирование для достижения оптимальной производительности
  Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.
- Операционные системы WindowsWindows: Минимальные требования к системе для систем Windows
  Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Windows, ознакомьтесь с требованиями к аппаратному и программному обеспечению.
- Windows: IBM Installation Manager
  IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.
- Windows: Контрольные списки для планирования сведений о сервере
  Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.
- Windows: Планирование мощностей
  Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.
- Windows: Практические рекомендации по именованию сервера
  Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.
- Windows: Каталоги установки
  К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

Windows: Что нужно знать в первую очередь

Перед первой установкой IBM Spectrum Protect необходимо собрать все сведения об используемых операционных системах, устройствах хранения данных, протоколах связи и системных конфигурациях.

Выпуски пакетов сервисного обслуживания сервера, программное обеспечение клиента и публикации есть по адресу: Портал поддержки IBM®.

Операционные системы WindowsОграничение: Установить и использовать сервер версии 8.1.5 в системе, в которой уже установлен компонент DB2 (независимо от того, был ли этот компонент DB2 установлен сам по себе или как часть какой-либо другой программы) нельзя. Для работы с сервером V8.1.5 нужно установить и использовать версию DB2, которая входит в пакет поставки сервера V8.1.5. В этой системе не должно существовать никаких других версий DB2.

Операционные системы WindowsСервер IBM Spectrum Protect можно установить на контроллере домена. Однако такой сервер может активно использовать процессор, что может воздействовать на другие приложения и приостановить их.

Опытные администраторы DB2 смогут выполнять сложные запросы SQL и использовать инструменты DB2 для мониторинга базы данных. Однако не следует использовать инструменты DB2 ни для изменения параметров конфигурации DB2, предварительно заданных IBM Spectrum Protect, ни для модификации среды DB2 для IBM Spectrum Protect какими-либо другими способами (как это допускается при работе с другими продуктами). Сервер V8.1.5 построен

и подвергнут расширенному тестированию с использованием языка определений данных (Data Definition Language - DDL) и конфигурации базы данных, которые внедряет сервер.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

Windows: Планирование для достижения оптимальной производительности

Прежде чем устанавливать сервер IBM Spectrum Protect, оцените характеристики и конфигурацию системы, чтобы убедиться, что сервер настроен для оптимальной производительности.

Процедура

1. Ознакомьтесь с разделом Windows: Что нужно знать в первую очередь.
2. Прочтите каждый из следующих подразделов.

- Windows: Планирование оборудования и операционной системы сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Windows: Планирование для дисков базы данных сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Windows: Планирование для дисков журнала восстановления сервера
  Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.
- Windows: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров
  Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.
- Windows: Планирование для пулов хранения на устройствах классов устройств DISK или FILE
  Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.
- Windows: Планирование правильного типа технологии хранения
  У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.
- Windows: Применение наилучших практических методов к установке сервера
  Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Windows: Планирование оборудования и операционной системы сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Соответствуют ли операционная система и оборудование требованиям или превышают их? • Число и частота процессоров • Системная память • Поддерживаемый уровень операционной системы	Если вы используете минимально необходимый объем памяти, вы можете поддерживать минимальную рабочую нагрузку. Вы можете поэкспериментировать, добавляя больше системной памяти, чтобы определить, повышается ли производительность. Затем решите, хотите ли вы оставить системную память выделенной для сервера. Проверьте различные вариации памяти, используя весь ежедневный цикл рабочей нагрузки сервера. Если у вас в системе работает несколько серверов, прибавьте требования для каждого сервера, чтобы получить требования к системе.	Прочтите требования к операционной системе в техническом замечании 1243309. Кроме того, смотрите рекомендации в документе Задачи по настройке для операционной системы и других приложений. Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Дополнительную информацию о том, как подобрать размер для сервера и хранения, смотрите в документе IBM Spectrum Protect Blueprint.
Сконфигурированы ли диски для оптимальной производительности?	Объем настройки, которую нужно производить для разных дисковых систем, различается. Убедитесь, что задана соответствующая глубина очереди и другие опции дисковых систем.	Дополнительные сведения смотрите в следующих разделах: • "Планирование для дисков базы данных сервера" • "Планирование для дисков журнала восстановления сервера" • "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли памяти на сервере?	Для более высоких рабочих нагрузок и таких дополнительных функций, как дедупликация данных и репликация узлов, требуется объем системной памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Для баз данных, не включенных для дедупликации данных, используйте следующие рекомендации по определению требований к системной памяти: • Для баз данных, объемом менее 500 ГБ, требуется 16 ГБ памяти. • Для баз данных, объемом от 500 ГБ до 1 ТБ, требуется 24 ГБ памяти. • Для баз данных, объемом от 1 ТБ до 1,5 ТБ, требуется 32 ГБ памяти. • Для баз данных, объем которых превышает 1,5 ТБ, требуется 40 ГБ памяти. Убедитесь, что вы выделили дополнительное пространство для активного и архивного журналов для обработки репликации.	Дополнительную информацию о требованиях при использовании этих возможностей, смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов • Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Есть ли в системе достаточное число адаптеров шины хоста (host bus adapter, HBA) для обработки операций с данными, которые сервер IBM Spectrum Protect должен выполнять одновременно?	Определите, для каких операций требуется использовать HBA одновременно. Например, серверу нужно сохранять 1 ГБ/сек данных резервных копий и при этом также нужно производить перенастройку пула хранения, для выполнения чего требуется 0,5 ГБ/сек. HBA должны быть способны обрабатывать все эти данные с нужной скоростью.	Смотрите раздел Настройка емкости HBA.
Превышает ли ширина полосы пропускания сети запланированную максимальную пропускную способность для резервнных копий?	Полоса пропускания сети должна позволять системе выполнять такие операции, как резервное копирование, когда это разрешено или соответствует обязательствам на уровне услуг. Для репликации узлов полоса пропускания сети должна быть больше запланированной максимальной пропускной способности.	Дополнительные сведения смотрите в следующих разделах: • Настройка производительности сети • Контрольный список по репликации узлов
Используете ли вы предпочтительную файловую систему для файлов сервера IBM Spectrum Protect?	Используйте файловую систему, обеспечивающую оптимальную производительность и доступность данных. Сервер использует прямой ввод-вывод для файловых систем, поддерживающих эту функцию. Использование прямого ввода-вывода может повысить пропускную способность и уменьшить степень использования процессора. Более подробную информацию о предпочтительной файловой системе для вашей операционной системы смотрите в документе Файловые системы, поддерживаемые сервером IBM Spectrum Protect.	Дополнительную информацию смотрите в разделе Конфигурирование операционной системы для производительности дисков.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы сконфигурировать достаточное пространство подкачки?	Пространство подкачки (или свопинга) расширяет память, доступную для обработки. Если объем свободной RAM в системе мал, программы или данные, которые не используются, перемещаются из памяти в пространство подкачки. Это действие высвобождает память для других операций, например, операций базы данных.  Операционные системы Windows Пространство подкачки конфигурируется автоматически.	

Windows: Планирование для дисков базы данных сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Находится ли база данных на быстрых дисках с низкой латентностью?	Не используйте для базы данных IBM Spectrum Protect следующие накопители: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Не используйте внутренние диска, включенные по умолчанию в большинство аппаратных компонентов серверов. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность. Если вы собираетесь использовать функции дедупликации данных в IBM Spectrum Protect, обратите внимание на производительность дисков в виде числа операций ввода-вывода в секунду (I/O operations per second, IOPS).	Дополнительную информацию смотрите в разделе Контрольный список для дедупликации данных.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Хранится ли база данных на дисках или LUN отдельно от дисков или LUN, используемых для активного журнала, архивного журнала и томов пула хранения?	Если отделить базу данных сервера от других серверных компонентов, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно. Совет: База данных и архивный журнал могут совместно использовать массив, когда вы применяете технологию твердотельных накопителей (solid-state drive, SSD).	
Если вы используете RAID, знаете ли вы, как выбрать оптимальный уровень RAID для вашей системы? Задаете ли вы все LUN одного и того же размера и типа RAID?	Если системе нужно производить большое число операций записи, RAID 10 превосходит RAID 5. Однако для RAID 10 требуется больше дисков, чем для RAID 5 при одном и том же объеме используемого пространства хранения. Если в вашей дисковой системе используется RAID, задайте все ваши LUN с использованием одного и того же размера и типа RAID. Например, не смешивайте 4+1 RAID 5 с 4+2 RAID 6.	
Если доступна опция задать размер полосы или размер сегмента, планируете ли вы оптимизировать размер при конфигурировании дисковой системы?	Если вы можете задать размер полосы или размер сегмента, используйте в дисковых системах для базы данных размер, равный 64 КБ или 128 КБ.	Размер блока, используемого для базы данных, зависит от табличного пространства. Большинство таблиц используют блоки по 8 КБ, но некоторые используют блоки по 32 КБ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Планируете ли вы создать хотя бы четыре каталога, которые также называются путями хранения, на четырех отдельных LUN для базы данных? Создайте по одному каталогу на отдельный массив в подсистеме. Если у вас менее трех массивов, создайте внутри массива отдельный том LUN.	При более высоких рабочих нагрузках и использовании некоторых функций требуется больше путей хранения, чем это соответствует минимальным требованиям. Такие операции сервера, как дедупликация данных, приводят к более высокому числу операций ввода-вывода в секунду (input/output operations per second, IOPS) для базы данных. Такие операции лучше выполняются, если у базы данных больше каталогов. В случае баз данных серверов, размер которых превышает 2 ТБ или которые, как ожидается, вырастут до этого размера, используйте восемь каталогов. При определении того, сколько путей хранения следует создать, рассмотрите запланированный рост системы. Сервер эффективнее использует высокое число путей хранения, если пути хранения присутствовали при первом создании сервера. Используйте переменную *DB2_PARALLEL_IO*, чтобы принудительно производить параллельный ввод-вывод в табличных пространствах, у которых один контейнер, или в табличных пространствах, контейнеры которых находятся более чем на одном физическом диске. Если вы не зададите переменную *DB2_PARALLEL_IO*, параллелизм ввода-вывода будет равен числу контейнеров, используемых табличным пространством. Например, если табличное пространство охватывает четыре контейнера, используемый уровень параллелизма ввода-вывода будет равен 4.	Дополнительные сведения смотрите в следующих разделах: • Контрольный список для дедупликации данных • Контрольный список по репликации узлов Справку относительно того, как предсказать рост, когда сервер производит дедупликацию данных, смотрите в техническом замечании 1596944. Последнюю информацию о размере базы данных, реорганизации базы данных и замечания относительно производительности для серверов IBM Spectrum Protect смотрите в техническом замечании 1683633. Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Является ли размер всех каталогов для базы данных одинаковым?	Каталоги одного и того же размера обеспечивают одинаковую степень параллелизма для операций базы данных. Если размер одного или нескольких каталогов для базы данных меньше размера остальных каталогов, то потенциал оптимизированного предварительного извлечения снизится. Эта рекомендация также применима, если вам нужно добавить пути хранения после первоначального конфигурирования сервера.	
Собираетесь ли вы увеличить глубину очереди для LUN базы данных в системах AIX?	Глубина очереди по умолчанию часто оказывается слишком мала.	Смотрите раздел Конфигурирование систем AIX для производительности диска.

Windows: Планирование для дисков журнала восстановления сервера

Используйте контрольный список, чтобы убедиться, что система, в которой установлен сервер, соответствует требованиям к конфигурации оборудования и программ.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Хранятся ли активный журнал и архивный журнал на дисках или на LUN отдельно от дисков или LUN, используемых для базы данных и томов пула хранения?	Убедитесь, что диски, на которых вы размещаете активный журнал, не используются для других задач сервера или системы. Не помещайте активный журнал на диски, содержащие базу данных сервера, архивный журнал или такие системные файлы, как пространство подкачки или свопинга.	Если отделить базу данных сервера, активный журнал и архивный журнал, это поможет сократить число конфликтов за одни и те же ресурсы среды различных операций, которые должны выполняться одновременно.
Находятся ли журналы на дисках с энергонезависимым кэшем записи?	Энергонезависимый кэш записи позволяет как можно быстрее записывать данные в журналы. Более быстрые операции записи для журналов могут повысить производительность операций сервера.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задаете ли вы для журналов размер, который адекватно поддерживает рабочую нагрузку?	Если вы не уверены относительно рабочей нагрузки, используйте самый большой возможный для вас размер. Активный журнал Максимальный размер - 512 ГБ, заданный с помощью опции сервера ACTIVELOGSIZE. Убедитесь, что у вас есть хотя бы 8 ГБ свободного пространства в файловой системе активного журнала после создания активных журналов фиксированного размера. Архивный журнал Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что размер архивного журнала, как минимум, равен размеру активного журнала.	• Подробную информацию о размерах журналов смотрите в информации о журнале восстановления в техническом замечании 1421060. • Информацию о подборе размеров при использовании дедупликации данных смотрите в разделе Контрольный список для дедупликации данных.
Задаете ли вы архивный журнал передачи управления при отказе? Размещаете ли вы этот журнал на диске, являющемся отдельным по сравнению с диском архивного журнала?	Архивный журнал передачи управления при отказе предназначен для использования сервером в аварийных ситуациях, когда архивный журнал переполняется. Для архивного журнала передачи управления при отказе можно использовать более медленные диски.	Используйте опцию сервера ARCHFAILOVERLOGDIRECTORY, чтобы указать расположение архивного журнала передачи управления при отказе. Отслеживайте использование каталога для архивного журнала передачи управления при отказе. Если архивный журнал передачи управления при отказе должен использоваться сервером, пространство архивного журнала может оказаться недостаточным.
Если вы производите зеркальное отображение активного журнала, используете ли вы только один тип зеркального отображения?	Зеркальное отображение журнала можно производить, используя один из описанных ниже методов. Используйте для журнала только один тип зеркального отображения. • Используйте опцию MIRRORLOGDIRECTORY, которая доступна для сервера IBM Spectrum Protect, чтобы задать расположение зеркального отображения. • Используйте в AIX зеркальное отображение программ, например, Logical Volume Manager (LVM). • Используйте зеркальное отображение на оборудовании дисковых систем.	Если вы зеркально отображаете активный журнал, убедитесь, что у дисков для активного журнала и зеркальной копии одинаковая скорость и надежность. Дополнительную информацию смотрите в разделе Конфигурирование и настройка журнала восстановления.

Windows: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров

Проверьте, как настроены пулы хранения каталогов-контейнеров и облачных контейнеров, чтобы убедиться, что они обеспечивают оптимальную производительность.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы быстрое дисковое хранения для базы данных IBM Spectrum Protect, если измерять ее в операциях ввода-вывода в секунду (input/output operations per second, IOPS)?	Используйте для базы данных высокопроизводительный диск. Используйте технологию твердотельных дисков для обработки дедупликации данных. Убедитесь, что база данных обеспечивает минимальное значение в 3000 IOPS. Для каждого терабайта данных, копируемого в день (до дедупликации данных) прибавьте к этому минимуму 1000 IOPS. Например, для сервера IBM Spectrum Protect, который пропускает 3 ТБ данных в день, потребуется 6000 IOPS для дисков базы данных: `минимум 3000 IOPS + 3000 (3 ТБ x 1000 IOPS) = 6000 IOPS`	Рекомендации относительно выбора диска смотрите в разделе "Планирование для дисков базы данных сервера". Дополнительные сведения об IOPS смотрите в документах IBM Spectrum Protect Макеты.
Достаточно ли памяти для размера вашей базы данных?	Для серверов IBM Spectrum Protect с размером базы данных, равным 100 ГБ, которые производят дедупликацию данных, используйте, как минимум, 40 ГБ системной памяти. Если сохраняемый объем данных резервных копий возрастает, может понадобиться увеличить требования к системной памяти. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память. Используйте больше памяти, чтобы улучшить кэширование страниц базы данных. Приведенные ниже рекомендация по размеру памяти основаны на ежедневном объеме новых данных, резервные копии которых вы создаете: • 128 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 1-2 ТБ • 192 ГБ системной памяти для ежедневных резервных копий данных, когда размер базы данных равен 2-4 ТБ	Требования к памяти

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Правильно ли вы подобрали размер емкости хранения для активного и архивного журналов базы данных?	Сконфигурируйте для сервера минимальный размер активного журнала 128 Гбайт, задав для опции сервера ACTIVELOGSIZE значение 131072. Рекомендуемый начальный размер архивного журнала - 1 ТБ. Размер архивного журнала ограничен размером файловой системы, в которой он находится, а не опцией сервера. Убедитесь, что для файловой системы есть хотя бы 10% дополнительного пространства на диске, превышающего размер архивного журнала. Используйте для архивных журналов баз данных каталог с начальной свободной емкостью, как минимум, 1 ТБ. Задайте каталог при помощи опции сервера ARCHLOGDIRECTORY. Определите пространство для архивного журнала восстановления после отказа при помощи опции сервера ARCHFAILOVERLOGDIRECTORY.	Дополнительную информацию о том, как подобрать размер системы, смотрите в документах IBM Spectrum Protect Макеты.
Включено ли сжатие для архивного журнала и резервных копий базы данных?	Включите опцию сервера ARCHLOGCOMPRESS, чтобы сэкономить пространство хранения. Эта опция сжатия отличается от строенного сжатия. Встроенное сжатие по умолчанию включено в IBM Spectrum Protect V7.1.5 и новее. Ограничение: Не используйте эту опцию, если объем резервных копий данных превышает 6 ТБ в день.	Дополнительную информацию о сжатии для вашей системы смотрите в документах IBM Spectrum Protect Макеты.
Расположены ли база данных и журналы IBM Spectrum Protect в разных томах диска (LUN)? Сконфигурирован ли диск, который используется для базы данных, в соответствии с рекомендациями для транзакционной базы данных?	База данных не должна использовать дисковые тома совместно с журналами или пулами хранения IBM Spectrum Protect, с другим приложением или с другой файловой системой.	Дополнительную информацию о базе данных сервера и конфигурации журнала восстановления смотрите в документе Конфигурирование и настройка базы данных сервера и журнала восстановления.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Используете ли вы, как минимум, восемь (2,2 ГГц или эквивалент) ядер процессора для каждого сервера IBM Spectrum Protect, который вы хотите использовать в сочетании с дедупликацией данных?	Если планируется использование дедупликации данных на стороне клиента, проверьте, есть ли у систем клиентов адекватные ресурсы, доступные во время операции резервного копирования, чтобы выполнять обработку дедупликации данных. Используйте процессор, эквивалентный по крайней мере одному процессорному ядру 2,2 ГГц, на каждый процесс резервного копирования с дедупликацией данных на стороне клиента.	• Эффективное планирование и использование дедупликации • IBM Spectrum Protect Макеты
Выделен ли вами достаточный объем пространства хранения для базы данных?	В первом приближении нужно запланировать выделение 100 ГБ для хранения базы данных на каждые 50 ТБ данных, которые будут защищены в дедуплицированных пулах хранения. *Защищенные данные* - это объем данных перед дедупликацией данных, включая все версии сохраненных объектов. Лучше всего задать новый пул хранения исключительно для дедупликации данных. Дедупликация данных производится на уровне пула хранения. Дедупликации подвергаются все данные, содержащиеся в пуле хранения, за исключением зашифрованных данных.	
Оценили ли вы емкость пула хранения для конфигурирования достаточного пространства, соответствующего размеру вашей среды?	Для оценки требований к емкости для дедуплицированного пула хранения можно использовать следующий метод: 1. Оцените базовый размер данных источника. 2. Оцените ежедневный размер резервных копий, используя предполагаемый темп изменений и роста. 3. Определите требования к сроку хранения. 4. Вычислите общий размер данных данных источника с учетом базового размера, ежедневного размера резервных копий и требований к сроку хранения. 5. Примените коэффициент дедупликации. 6. Примените коэффициент сжатия. 7. Округлите оценку, чтобы учесть переходное использование пула хранения.	Пример использования этого метода смотрите на веб-странице Эффективное планирование и использование дедупликации.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Распределили ли вы операции дискового ввода-вывода по нескольким дисковым устройствам и контроллерам?	Используйте массивы, которые состоят из как можно большего количества дисков (иногда это называется 'широкое чередование'. Убедитесь, что вы используете один каталог базы данных для отдельного массива в подсистеме. Задайте переменную реестра *DB2_PARALLEL_IO*, так чтобы включить параллельный ввод-вывод для каждого табличного пространства, используемого, если контейнеры в табличном пространстве охватывают несколько физических дисков. Если полоса пропускания для ввода-вывода доступна, а размер файлов велик (например, 1 МБ), процесс нахождения дубликатов может использовать ресурсы всего процессора. Когда файлы меньше, более критичны другие узкие места. Задайте восемь или больше файловых систем для класса устройств дедуплицированного пула хранения, чтобы операции ввода-вывода распределялись по максимально возможному числу LUN и физических устройств.	Рекомендации по настройке пулов хранения смотрите в разделе "Планирование для пулов хранения на устройствах классов устройств DISK или FILE". Информацию о настройке переменной *DB2_PARALLEL_IO* смотрите в документе Рекомендуемые параметры для переменных реестра IBM DB2.
Запланировали ли вы ежедневные операции на основе вашей стратегии резервного копирования?	Наилучшая последовательность операций будет следующей: 1. Резервное копирование клиента 2. Защита пула хранения 3. Репликация узлов 4. Резервное копирование базы данных 5. Окончание действия устаревших файлов	• Планирование дедупликации данных и процессов репликации узла • Ежедневные операции для пулов хранения каталогов-контейнеров

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Достаточно ли у вас пространства хранения для управления списком блокировки DB2?	Если выполняется дедупликация данных, в состав которых входят большие объекты или большое число одновременно обрабатываемых файлов, процесс может привести к тому, что станет не хватать пространства хранения. При нехватке пространства хранения списка блокировок могут происходить ошибки резервного копирования, отказы процессов управления данными или перерывы в работе сервера. Если дедупликация данных обрабатывает файлы размером более 500 ГБ, это вероятнее всего приведет к истощению пространства хранения. Но если большое число выполняемых операций резервного копирования использует дедупликацию данных на стороне клиента, эта проблема может также произойти и с файлами меньшего размера.	Информацию о настройке параметра DB2 LOCKLIST смотрите в документе Настройка дедупликации данных на стороне сервера.
Доступна ли достаточная полоса пропускания для передачи данных на сервер IBM Spectrum Protect?	Чтобы переносить данные на сервер IBM Spectrum Protect, используйте дедупликацию данных на стороне клиента или на стороне сервера и сжатие, чтобы уменьшить необходимую ширину полосы пропускания. Используйте сервер V7.1.5 или новее, чтобы применить встроенное сжатие, и используйте клиент V7.1.6 или новее, чтобы включить усовершенствованную обработку сжатия.	Дополнительные сведения смотрите в описании опции клиента enablededup.
Определили ли вы, сколько каталогов пула хранения следует назначить для каждого пула хранения?	Назначьте каталоги для пула хранения, используя команду DEFINE STGPOOLDIRECTORY. Создайте несколько каталогов пула хранения и убедитесь, что для каждого каталога создается резервная копия на отдельном дисковом томе (LUN).	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Выделен ли вами достаточный объем дискового пространства в пуле хранения облачных контейнеров?	Чтобы предотвратить ошибки резервного копирования, убедитесь, что в локальном каталоге достаточно места. Оптимальный размер дискового пространства указан ниже в списке: • Для SCSI с последовательным подключением (SAS) и вращающегося диска вычислите объем новых данных, ожидаемых поле ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства. • Для систем хранения на основе флэш-памяти, у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 3 Тбайт. • Для систем хранения с твердотельными накопителями (SSD), у которых есть быстрые сетевые соединения с высокопроизводительными облачными системами, требуется 5 Тбайт.	

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация

Выбрали ли вы подходящий тип локальной системы хранения?	Убедитесь, что передача данных из локальной системы хранения в облако завершена до начала следующего цикла резервного копирования.
	Совет: Данные удаляются из локальной системы хранения вскоре после их перемещения в облако.
	Учтите следующие рекомендации:
	• Используйте флеш-память или твердотельные накопители (SSD) для больших облачных система высокой производительности. Убедитесь, что у вас есть ссылка на глобальную сеть (wide area network, WAN) с выделенными 10 Гбайт памяти и высокоскоростным соединением с хранилищем объектов. Например, используйте флеш-память или SSD, если у вас выделенная ссылка 10 ГБ WAN плюс высокоскоростное соединение либо с расположением IBM® Cloud Object Storage, либо с центром данных Amazon Simple Storage Service (Amazon S3).
	• Для указанных ниже сценариев используйте диски SAS большей емкости 15000 rpm:
	  ○ Системы среднего размера
	  ○ Медленные соединения с облаком, например 1 Гбайт
	  ○ При использовании IBM Cloud Object Storage в качестве провайдера службы в нескольких регионах
	• Для SAS или вращающегося диска вычислите объем новых данных, ожидаемых после ежедневного сокращения объема данных (сжатие и дедупликация данных). Выделите до 100 процентов этого количества в терабайтах для дискового пространства.	

Windows: Планирование для пулов хранения на устройствах классов устройств DISK или FILE

Используйте контрольный список, чтобы проверить, как настроены дисковые пулы хранения. Этот контрольный список содержит советы для пулов хранения, использующих классы устройств DISK или FILE.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Могут ли LUN пула хранения поддерживать пропускную способность для последовательного чтения и записи, объемом 256 КБ, чтобы адекватно обрабатывать рабочую нагрузку в пределах ограничений времени?	При планировании пиковых нагрузок учитывайте все данные, которые сервер должен читать из дисковых пулов хранения или записывать в дисковые пулы хранения одновременно. Например, рассмотрим пиковый поток данных от одновременно выполняющихся операций резервного копирования клиента и операций по перемещению данных сервером, например, перенастройку. В подавляющем большинстве случаев сервер IBM Spectrum Protect производит чтение из пулов хранения и записывает данные в пулы хранения блоками по 156 КБ. Если дисковая система обеспечивает такую возможность, сконфигурируйте дисковую систему для оптимальной производительности при выполнении последовательных операций чтения/записи, а не случайных операций чтения/записи.	Дополнительную информацию смотрите в документе Анализ базовой производительности дисковых систем.
Сконфигурирован ли диск для использования кэша чтения и записи?	Используйте больший объем кэша, чтобы повысить производительность.	
Определили ли вы правильный размер, который следует использовать для томов пула хранения, когда пулы хранения используют класс устройств FILE?	Ознакомьтесь с информацией в разделе Оптимальное число и размер томов для пулов хранения, использующих диск. Если у вас нет информации, которая бы позволила оценить размер томов класса устройств FILE, начните с томов, имеющих 50 ГБ.	Как правило, проблемы чаще возникают, если тома слишком малы. Если тома больше, чем требуется, сообщается о малом числе проблем. Когда вы определите размер тома, который следует использовать, в качестве предосторожности выберите размер, который может оказаться больше необходимого.
Используете ли вы заранее выделенные тома для пулов хранения, использующих классы устройств FILE?	Чистые тома могут вызвать фрагментацию файлов. Чтобы убедиться, что пулу хранения будет хватать томов, задайте для параметра MAXSCRATCH значение больше нуля.	Используйте серверную команду DEFINE VOLUME, чтобы заранее выделить тома в пуле хранения. Используйте серверную команду DEFINE STGPOOL или UPDATE STGPOOL, чтобы задать параметр MAXSCRATCH.
Сравнивали ли вы максимальное число сеансов клиентов с числом заданных томов для пулов хранения, использующих классы устройств FILE?	Всегда оставляйте в пулах хранения достаточное число пригодных для использования томов, чтобы разрешить одновременное выполнение ожидаемого пикового числа сеансов клиентов. Тома могут быть чистыми, пустыми или частично заполненными томами.	В случае пулов хранения, которые используют класс устройств FILE, на том одновременно может производить запись только один сеанс или процесс.

Вопрос	Задачи, характеристики, опции или параметры	Дополнительная информация
Задали ли вы для параметра MOUNTLIMIT класса устройств достаточно высокое значение, чтобы учесть число томов, которые могут быть смонтированы параллельно, когда пулы хранения используют класс устройств FILE?	Для пулов хранения, использующих дедупликацию данных, параметр MOUNTLIMIT, как правило, находится в диапазоне 500-1000. Задайте для MOUNTLIMIT значение, равное максимальному числу необходимых точек монтирования, необходимых для всех активных сеансов. Рассмотрим параметры, которые влияют на максимальное число необходимых точек монтирования: • Опция сервера MAXSESSIONS, представляющая собой максимальное число сеансов IBM Spectrum Protect, которые могут выполняться одновременно. • Параметр MAXNUMMP, указывающий, какое максимальное число точек монтирования может использовать каждый клиентский узел. Например, если максимальное число сеансов резервного копирования клиентских узлов, как правило, составляет 100, а для каждого из узлов задан параметр `MAXNUMMP=2`, умножьте 100 узлов на 2 точки монтирования для каждого узла, чтобы получить значение 200 для параметра MOUNTLIMIT.	Используя серверную команду REGISTER NODE или UPDATE NODE, задайте параметр MAXNUMMP для клиентских узлов.
Определили ли вы, сколько томов пула хранения поместить в каждую файловую систему для пулов хранения, использующих классы устройств DISK?	То, как вы конфигурируете пространство хранения для пула хранения, использующего класс устройств DISK, зависит от того, используете ли вы RAID для дисковой системы. Если вы не используете RAID, сконфигурируйте по одной файловой системе на физический диск и задайте по одному тому пула хранения для каждой файловой системы. Если вы используете RAID 5 с *n*+1 томами, сконфигурируйте пространство хранения одним из следующих способов: • Сконфигурируйте *n* файловых систем на LUN и задайте по одному тому пула хранения для файловой системы. • Сконфигурируйте одну файловую систему и *n* томов пула хранения для LUN.	Пример схемы, соответствующей этой рекомендации, смотрите в документе Пример схемы пулов хранения сервера.
Создали ли вы пулы хранения для распределения операций ввода-вывода по нескольким файловым системам?	Убедитесь, что каждая файловая система находится на отдельном LUN в дисковой системе. Как правило, 10-30 файловых систем - это оптимальная цель, но вы должны убедиться, что размер файловых систем будет не менее, чем 250 ГБ (примерно).	Дополнительные сведения смотрите в следующих разделах: • Настройка дискового хранения для сервера • Настройка и конфигурирование пулов хранения и томов

Windows: Планирование правильного типа технологии хранения

У устройств хранения разные характеристики емкости и производительности. Эти характеристики влияют на то, какие устройства лучше всего использовать в сочетании с IBM Spectrum Protect.

Процедура

Ознакомьтесь со следующей таблицей, которая поможет вам выбрать правильный тип технологии хранения для ресурсов хранения, необходимых серверу.

Табл. 1. Типы технологии хранения в требованиях по хранению IBM Spectrum Protect

Тип технологии хранения	**Database**	**Активный журнал**	**Архивный журнал и резервный архивный журнал**	**Пулы хранения**
Твердотельный диск (Solid-state disk, SSD)	Размещайте базу данных на SSD при следующих обстоятельствах: • Вы используете дедупликацию данных IBM Spectrum Protect. • Вы ежедневно производите резервное копирование более чем 8 ТБ новых данных.	Если вы поместите базу данных IBM Spectrum Protect на SSD, лучше всего поместить активный журнал на SSD. Если пространство недоступно, используйте вместо этого высокопроизводит. диск.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Архивный журнал и архивные журналы передачи управления при отказе можно поместить на носители с более медленными типами технологии хранения.	Оставьте накопители SSD для использования в сочетании с базой данных и активным журналом. Пулы хранения можно поместить на носители с более медленными типами технологии хранения.
Высокопроизв. диск со следующими хар-ками: • **Диск 15 К rpm** • **Оптоволокно (Fibre Channel) интерфейс или последов. подкл. интерфейс SCSI (SAS).**	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Используйте высокопроизв. диски при следующих обстоятельствах: • Сервер не производит дедупликацию данных. • Сервер не производит репликацию узлов. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Высокопроизв. диски можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте высокопроизв. диски для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.

Тип технологии хранения	Database	Активный журнал	Архивный журнал и резервный архивный журнал	Пулы хранения
Диск средней произв. или высокопроизв. диск со следующими хар-ками: • **Диск 10 K rpm** • **Оптоволокно (Fibre Channel) интерфейс или интерфейс SAS**	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Изолируйте базу данных сервера от ее журналов и пулов хранения и от данных для других приложений.	Если дисковая система представляет собой смесь дисковых технологий, используйте более быстрые диски для базы данных и активного журнала. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте активный журнал от базы данных сервера, от архивных журналов и пулов хранения.	Диск средней производительности или высокопроизв. диск можно использовать для архивного журнала и архивных журналов передачи управления при отказе. Чтобы обеспечить доступность, изолируйте эти журналы от базы данных и активного журнала.	Используйте диск средней производительности или высокопроизв. диск для пулов хранения при следующих обстоятельствах: • Данные часто читаются. • Данные часто записываются. Чтобы обеспечить достаточный уровень производительности и доступности, изолируйте данные пула хранения от базы данных сервера и от данных для других приложений.
SATA, пространство хранения, подключенное к сети	Не используйте этот тип хранения для базы данных. Не помещайте базу данных в системы хранения XIV.	Не используйте этот тип хранения для активного журнала.	Использование этой более медленной технологии хранения является приемлемым, так как эти журналы записываются один раз и редко читаются.	Используйте эту более медленную технологию хранения при следующих обстоятельствах: • Данные редко записываются, например, записываются один раз. • Данные редко читаются. .
Лента и виртуальная лента				Используйте для долгосрочного хранения, если данные используются нечасто.

Windows: Применение наилучших практических методов к установке сервера

Как правило, конфигурация и выбор оборудования оказывают наиболее значительное влияние на производительность решения IBM Spectrum Protect. Другими факторами, влияющими на производительность, являются выбор и конфигурация операционной системы, а также конфигурация IBM Spectrum Protect.

Процедура

- Описанные ниже наилучшие методы являются наиболее важными для достижения оптимальной производительности и предотвращения ошибок.
- Смотрите таблицу, чтобы определить наилучшие методы, применимые к вашей среде.

Практическая рекомендация	Дополнительная информация
Используйте для базы данных сервера быстрые диски. Твердотельные диски (solid-state disks, SSD) уровня предприятия с оптоволоконным интерфейсом или интерфейсом SAS предлагают наивысшую производительность.	Используйте для базы данных быстрые диски с низкой латентностью. Использование SSD является существенным, если вы используете дедупликацию данных и репликацию узлов. Старайтесь не использовать диски Serial Advanced Technology Attachment (SATA) и Parallel Advanced Technology Attachment (PATA). Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование правильного типа технологии хранения"
Убедитесь, что в системе сервера достаточно памяти.	Прочтите требования к операционной системе в техническом замечании 1243309. При более высоких рабочих нагрузках требуется больше ресурсов, чем указано в минимальных требованиях. Такие дополнительные функции, как дедупликация данных и репликация узлов, могут потребовать объем памяти, превышающий минимальный объем, указанный в документе с требованиями к системе. Если вы планируете запускать несколько экземпляров сервера, каждому экземпляру потребуется объем памяти, указанный для одного сервера. Умножьте объем памяти для одного сервера на число экземпляров, которые вы собираетесь запускать в системе.
Отделите базу данных сервера, активный журнал, архивный журнал и дисковые пулы хранения друг от друга.	Держите все ресурсы хранения IBM Spectrum Protect на отдельных дисках. Держите диски пулов хранения храниться отдельно от дисков базы данных сервера и журналов. Операции пулов хранения могут перекрываться операциями базы данных, если они находятся на одних и тех же дисках. В идеале база данных сервера и журналы также должны быть отделены друг от друга. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ "Планирование для дисков базы данных сервера" ○ "Планирование для дисков журнала восстановления сервера" ○ "Планирование для пулов хранения на устройствах классов устройств DISK или FILE"
Используйте для базы данных сервера хотя бы четыре каталога. Для больших серверов или серверов, использующих дополнительные функции, используйте восемь каталогов.	Поместите каждый каталог на LUN, изолированный от других LUN и от других приложений. Сервер считается большим, если его база данных превышает 2 ТБ или если ожидается, что она вырастет больше этого размера. Используйте для таких серверов восемь каталогов. Смотрите раздел "Планирование для дисков базы данных сервера".
Если вы используете дедупликацию данных и/или репликацию узлов, следуйте рекомендациям по конфигурированию базы данных и других элементов.	Сконфигурируйте базу данных сервера в соответствии с рекомендациями, так как база данных чрезвычайно важна для того, чтобы сервер смог хорошо работать, если используются такие функции. Подробную информацию и дополнительные советы смотрите в следующих разделах: ○ Контрольный список для дедупликации данных ○ Контрольный список по репликации узлов

Практическая рекомендация	Дополнительная информация
В случае пулов хранения, которые используют класс устройств типа FILE, выполните рекомендации по размеру томов пула хранения. Как правило, тома 50 ГБ подходят лучше всего.	Прочтите информацию в разделе Оптимальное число и размер томов для пулов хранения, использующих диск, чтобы это помогло вам определить размер тома. Сконфигурируйте устройства пула хранения и файловые системы на основе требований к пропускной способности, а не только на основе требований к емкости. Изолируйте устройства хранения, используемые продуктом IBM Spectrum Protect, от других приложений с высоким объемом ввода-вывода и убедитесь, что для этого хранилища обеспечивается достаточная пропускная способность. Дополнительные сведения смотрите в разделе Контрольный список для пулов хранения на устройствах DISK или FILE.
Запланируйте операции клиента IBM Spectrum Protect и действия по обслуживанию сервера, чтобы избежать перекрывания операций или свести такое перекрывание к минимуму.	Дополнительные сведения смотрите в следующих разделах: ◦ Настройка расписания для ежедневных операций ◦ Контрольный список для конфигурации сервера
Постоянно осуществляйте мониторинг операций.	Проводя мониторинг, вы сможете раньше находить ошибки и вам будет проще выявлять их причины. Срок хранения записей отчетов мониторинга может доходить до года - это поможет вам выявлять тенденции и планировать рост. Смотрите раздел Мониторинг среды и ее обслуживание с целью обеспечения производительности.

Windows: Минимальные требования к системе для систем Windows

Прежде чем устанавливать сервер IBM Spectrum Protect в операционной системе Windows, ознакомьтесь с требованиями к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению для установки сервера IBM Spectrum Protect

Оптимальная среда IBM Spectrum Protect настраивается с дедупликацией данных с использованием IBM Spectrum Protect Blueprints.

Самую последнюю информацию о требованиях к системе IBM Spectrum Protect смотрите в техническом замечании 1243309.

Windows: IBM Installation Manager

IBM Spectrum Protect использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке IBM Spectrum Protect. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать IBM Spectrum Protect.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение
: Устанавливаемый модуль программного продукта.

  Предложение IBM Spectrum Protect содержит все носители, которые требуются IBM Installation Manager для установки IBM Spectrum Protect.

Пакет
: Группа программных компонентов, необходимых для установки предложения.
Пакет IBM Spectrum Protect включает в себя следующие компоненты:

- Программа установки IBM Installation Manager
- Предложение IBM Spectrum Protect

Группа пакетов
: Набор пакетов, использующих общий родительский каталог.

Группа пакетов по умолчанию для пакета IBM Spectrum Protect - `IBM Installation Manager`.

Репозиторий
: Удаленная или локальная область хранения данных и других ресурсов программы.

Пакет IBM Spectrum Protect хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
: Каталог, содержащий файлы или подключаемые модули программ, которые совместно используются пакетами.

IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии IBM Spectrum Protect.

Windows: Контрольные списки для планирования сведений о сервере

Контрольные списки помогут вам спланировать объем и расположение пространства хранения, необходимого серверу IBM Spectrum Protect. Их можно использовать также для сохранения трассировки имен и ID пользователей.

Операционные системы WindowsОграничение: Если используется файловая система File Allocation Table (FAT или FAT32) или формат New Technology File System (NTFS), задать корневой каталог системы в качестве каталога базы данных или журнала нельзя. Нужно создать в корневом каталоге один или несколько подкаталогов. После этого создайте в подкаталогах каталоги базы данных и журнала.

Элемент	**Необходимое пространство**	**Число каталогов**	**Положение каталогов**
База данных			
Активный журнал			
Архивный журнал			
Необязательно: Зеркальная копия активного журнала			
Необязательно: Вторичный архивный журнал (резервный каталог для архивного журнала)			

Элемент	**Имена и ID пользователей**	**Расположение**
ID пользователя экземпляра для сервера, то есть ID, который использовался для запуска и работы сервера IBM Spectrum Protect		
Домашний каталог для сервера, то есть каталог, содержащий ID пользователя экземпляра		
Имя экземпляра базы данных		

Элемент	Имена и ID пользователей	Расположение
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)		
Имя сервера; для каждого сервера используйте уникальное имя		

Windows: Планирование мощностей

Планирование емкости для IBM Spectrum Protect включает в себя управление такими ресурсами, как база данных, журнал восстановления и совместно используемая область ресурсов. Для максимального увеличения ресурсов как части планирования мощности необходимо оценить требования к пространству для базы данных и журнала восстановления. В области совместно используемых ресурсов должно быть достаточно пространства для каждой установки или обновления.

- Windows: Оценка необходимого объема пространства для базы данных
  Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.
- Windows: Требования к пространству журнала восстановления
  В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.
- Windows: Мониторинг использования пространства для базы данных и журналов восстановления
  Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.
- Windows: Удаление файлов отката установки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Windows: Оценка необходимого объема пространства для базы данных

Оценить необходимое для базы данных пространство можно, исходя из максимально допустимого числа файлов, одновременного находящихся в хранилище сервера, или на основе емкости пула хранения.

Об этой задаче

В качестве начального объема пространства базы данных можно порекомендовать использовать не менее 25 ГБ. Доступ к пространству файловой системы предоставляется должным образом. Размер базы данных 25 ГБ достаточен для среды тестирования или среды, включающей только менеджер библиотек. Для производственного сервера с поддержкой клиентских рабочих нагрузок размер базы данных должен быть больше. Если вы используете дисковые пулы хранения с произвольным доступом (DISK), потребуется дополнительное пространство хранения баз данных и журналов для пулов хранения с последовательным доступом.

Максимальный размер базы данных IBM Spectrum Protect - 6 ТБ.

Информацию об оценке размера базы данных в производственной среде на основе числа файлов и размера пула хранения смотрите в темах ниже.

- Windows: Оценка требований к пространству базы данных на основе числа файлов
  Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.

- Windows: Оценка требований к пространству базы данных на основе мощности пула хранения
  Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.
- Windows: Менеджер баз данных и временное пространство
  Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Windows: Оценка требований к пространству базы данных на основе числа файлов

Если возможно оценить максимальное количество файлов, которые будут одновременно находиться в системе хранения сервера, это число можно использовать для оценки требований к пространству базы данных.

Об этой задаче

Для оценки требований к объему пространства на основе максимального числа файлов в системе хранения сервера используйте следующие рекомендации:

- 600 - 1000 байт на каждую хранимую версию файла, включая резервные копии образов.
  Ограничение: Сюда не входит пространство, используемое во время дедупликации данных.
- 100 - 200 байт на каждый кэшированный файл, файл пула хранения копий, файл пула активных данных и дедуплицированный файл.
- Дополнительное пространство требуется для оптимизации базы данных в части поддержки переменных схем доступа к данным и внутренней обработки данных на сервере. Объем дополнительного пространства равен 50% оцененного размера памяти для хранения файловых объектов.

В следующем примере для единственного клиента вычисления основываются на максимальных значениях из предыдущих инструкций. В примерах не учитывается возможное использование объединения файлов. В общем случае объединение файлов сокращает объем требуемого пространства базы данных. Объединение файлов не затрагивает перенесенные файлы.

Процедура

1. Вычислите число версий файлов. Чтобы получить число версий файлов, сложите следующие значения:
   a. Вычислите число резервных копий файлов. Например, одновременно может существовать до 500 000 резервных копий клиентских файлов. В этом примере политики хранения требуют, чтобы хранилось до трех резервных копий каждого файла:

      ```
      500 000 файлов * 3 копии = 1 500 000 файлов
      ```

   b. Вычислите количество архивных файлов. Например, до 100 000 клиентских файлов могут быть архивными копиями.
   c. Вычислите количество перенесенных файлов. Например, до 200 000 клиентских файлов могут быть перемещены с клиентских рабочих станций.

   Если для каждого файла требуется 1000 байт, то общий объем требуемого для принадлежащих клиентам файлов пространства базы данных - 1,8 ГБ.

   ```
   (1 500 000 + 100 000 + 200 000) * 1000 = 1,8 ГБ
   ```

2. Вычислите число кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов:
   a. Вычислите количество кэшированных копий. Например, кэширование разрешено в дисковом пуле хранения размером 5 ГБ. Верхний порог переноса пула равен 90%, а нижний - 70%. Таким образом, 20% дискового пула, то есть 1 ГБ, будет занято кэшированными файлами.
   Если средний размер файла около 10 КБ, в кэше в любой момент времени находится около 100000 файлов:

      ```
      100 000 файлов * 200
      байт = 19 МБ
      ```

b. Вычислите количество файлов пула хранения копий. Для всех основных пулов памяти создается резервная копия:

```
(1 500 000 + 100 000 + 200 000) * 200 байт = 343 МБ
```

c. Вычислите количество активных файлов пула хранения. Все данные активных резервных копий клиента в первичных пулах хранения копируются в пул хранения активных данных. Допустим, что 500 000 версий 1 500 000 резервных копий файлов в основном пуле являются активными:

```
500 000 * 200 байт = 95 МБ
```

d. Вычислите количество дедуплицированных данных. Допустим, что пул хранения данных, подвергнутых дедупликации, содержит 50000 файлов:

```
50 000 * 200 байт = 10 МБ
```

На основании этих вычислений для клиентских кэшированных файлов, файлов пула хранения копий, файлов пула активных данных и дедуплицированных файлов требуется примерно 0,5 ГБ дополнительного пространства базы данных.

3. Вычислите объем дополнительного пространства, требуемый для оптимизации базы данных. Для обеспечения оптимального доступа к данным и управления сервером требуется дополнительное пространство базы данных. Объем дополнительного пространства базы данных равен 50% общего пространства, необходимого для хранения файловых объектов.

```
(1,8 + 0,5) * 50% = 1,2 ГБ
```

4. Вычислите общий объем пространства базы данных, требуемый для этого клиента. Общий объем составит примерно 3,5 ГБ:

```
1,8 + 0,5 + 1,2 = 3,5 ГБ
```

5. Вычислите общий объем пространства базы данных, требуемый для всех клиентов. Если предыдущие оценки приведены для типичного клиента и у вас 500 таких клиентов, то можно использовать для примера следующую оценку общего объема пространства базы данных, требуемого для всех клиентов:

```
500 * 3,5 = 1,7 ТБ
```

Результаты

Совет: В приведенных выше примерах результаты представляют собой примерные оценки. Фактический размер базы данных может отличаться от ожидаемого из-за таких факторов, как число каталогов и длина полных имен файлов. Рекомендуется периодически производить мониторинг базы данных и корректировать ее размер, если потребуется.

Дальнейшие действия

При обычных операциях серверу IBM Spectrum Protect может потребоваться временное пространство баз данных. Это пространство необходимо для следующих задач:

- Сохранять результаты сортировки или упорядочивания, которые еще не сохранены и не оптимизированы непосредственно в базе данных. Эти результаты временно сохраняются в базе данных для обработки.
- Предоставлять административный доступ к базе данных одним из следующих способов:
  - Через клиент Open Database Connectivity (ODBC) DB2
  - Через клиент Oracle Java™ Database Connectivity (JDBC)
  - Из командной строки клиента администрирования на сервер с помощью Structured Query Language (SQL)

Используйте дополнительные 50 ГБ временного пространства на каждые 500 ГБ пространства для файловых объектов и оптимизации. Смотрите инструкции в следующей таблице. В примере, использованном в предыдущем шаге, для файловых объектов и оптимизации для 500 клиентов требуется общий объем пространства базы данных 1,7 ТБ. На основании этих оценок еще около 200 ГБ требуется для временного пространства. Суммарный объем требуемого пространства базы данных составляет 1,9 ТБ.

Размер базы данных	Минимальные потребности временного пространства
< 500 ГБ	50 ГБ
≥ 500 ГБ и < 1 ТБ	100 ГБ

Размер базы данных	Минимальные потребности временного пространства
≥ 1 ТБ и < 1,5 ТБ	150 ГБ
≥ 1,5 и < 2 ТБ	200 ГБ
≥ 2 и < 3 ТБ	250 - 300 ГБ
≥ 3 и < 4 ТБ	350 - 400 ГБ

Windows: Оценка требований к пространству базы данных на основе мощности пула хранения

Чтобы оценить требования к пространству базы данных на основе мощности пула хранения, используйте коэффициент 1 - 5%. Например, если вам требуется мощность пула хранения в 200 ТБ, размер базы данных составит примерно 2 - 10 ТБ. Как общее правило, сделайте вашу базу данных настолько большой, насколько это возможно, чтобы предотвратить недостаток памяти. Если в пространстве базы данных не хватит памяти, может произойти сбой операций сервера и операций сохранения, выполняемых клиентом.

Windows: Менеджер баз данных и временное пространство

Менеджер баз данных сервера IBM Spectrum Protect выделяет системную память и дисковое пространство для базы данных и управляет ими. Объем нужного пространства базы данных зависит от объема доступной памяти системы и рабочей нагрузки сервера.

Менеджер баз данных сортирует данные в определенном порядке, как в операторе SQL, который вводится для запроса данных. В зависимости от рабочей нагрузки на сервере, если объем данных больше, чем может обрабатывать менеджер баз данных, эти упорядоченные данные размещаются во временном дисковом пространстве. Данные располагаются во временном дисковом пространстве, когда уже существует большой набор результатов. Менеджер баз данных динамически управляет памятью, используемой при размещении данных во временном дисковом пространстве.

Например, большой объем результатов может возникнуть при обработке устаревания данных. Если памяти системы недостаточно для хранения набора результатов, некоторые данные размещаются во временной дисковом пространстве. Если во время обработки устаревания выбран чрезмерно большой узел или файловое пространство, то менеджер баз данных не сможет отсортировать данные в памяти. Для сортировки данных менеджеру баз данных понадобится временное пространство.

Чтобы запустить операции базы данных, рассмотрите возможность добавления пространства базы данных для следующих сценариев:

- У базы данных маленький объем пространства, и операции сервера, которым требуется временное пространство, используют оставшуюся незанятую память.
- Файловые пространства велики, или для них назначена политика, которая создает много версий файлов.
- Сервер IBM Spectrum Protect должен быть запущен с ограниченным объемом памяти. Для запуска своих операций база данных использует главную память сервера IBM Spectrum Protect. Однако если памяти недостаточно, сервер IBM Spectrum Protect выделяет для базы данных временное пространство на диске. Например, если доступно 10 ГБ памяти, а для операций базы данных требуется 12 ГБ, база данных использует временное пространство.
- При внедрении сервера IBM Spectrum Protect появится сообщение об ошибке `недостаток памяти базы данных`. Отслеживайте в активном журнале сервера сообщения, относящиеся к пространству баз данных.

Важное замечание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами Fix Pack IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, чтобы не повредить базу данных.

Windows: Требования к пространству журнала восстановления

В IBM Spectrum Protect термин *журнал восстановления* включает в себя активных журнал, архивный журнал, зеркальную копию активного журнала и архивный журнал восстановления при отказе. Требуемый объем пространства для журнала восстановления зависит от различных факторов, например, от интенсивности операций клиента на сервере.

- Windows: Пространство активных и архивных журналов
  Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных

страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.

- Windows: Пространство зеркальной копии активного журнала
  Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.
- Windows: Пространство резервного архивного журнала
  Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Windows: Пространство активных и архивных журналов

Оценивая необходимый размер памяти для активного и архивного журналов, включите несколько дополнительных страниц на случай непредвиденных обстоятельств, например, случайных тяжелых рабочих нагрузок и восстановления после сбоя.

Максимальный размер активного журнала для серверов IBM Spectrum Protect версии 7.1 и новее должен составлять 512 ГБ. Размер архивного журнала ограничен размером файловой системы, в которой он установлен.

Учитывайте следующие общие рекомендации для оценки размера активного журнала:

- Рекомендуемый начальный размер активного журнала - 16 Гбайт.
- Убедитесь, что размер активного журнала достаточен, по крайней мере, для тех текущих операций, которые обычно обрабатываются сервером. В качестве меры предосторожности попытайтесь учесть наибольший объем работы, которую сервер может выполнять единовременно. Обеспечьте для активного журнала некоторый дополнительный объем пространства, которое может использоваться при необходимости. Предусмотрите 20% дополнительного пространства.
- Отслеживайте используемое и доступное пространство активного журнала. При необходимости подстраивайте размер активного журнала в зависимости от таких факторов, как активность клиентов и уровень операций сервера.
- Убедитесь, что размер каталога, в котором содержится активный журнал, не меньше размера самого журнала. Если каталог больше по размеру, чем активный журнал, при необходимости он может использоваться для обработки аварийного восстановления.
- Убедитесь, что в файловой системе, которая содержит каталог активного журнала, есть по крайней мере 8 Гбайт свободного места для требований временных перемещений журналов.

Рекомендуемый начальный размер архивного журнала - 48 Гбайт.

Каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала, сгенерированные с момента последнего полного резервного копирования. Например, если вы производите резервное копирование базы данных ежедневно, каталог архивного журнала должен быть достаточно большим, чтобы в нем уместились файлы журнала для всех операций клиентов в течение 24 часов. Чтобы освободить пространство, при полном резервном копировании базы данных сервер удаляет устаревшие файлы архивного журнала. Если каталог архивного журнала переполняется, а каталог резервного архивного журнала не существует, файлы журнала остаются в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением каталога активного журнала. При повторном запуске сервера часть используемого для активного журнала пространства освобождается.

После установки сервера вы можете отслеживать использование архивного журнала и пространство каталога архивного журнала. Если каталог архивного журнала переполняется, то это может привести к следующим проблемам:

- Сервер не сможет провести полное резервное копирование базы данных. Исследуйте и разрешите эту проблему.
- Другие приложения, выполняют запись в каталог архивного журнала, уменьшая объем доступного для архивного журнала пространства. Не используйте пространство архивного журнала для других прикладных программ, в том числе для других серверов IBM Spectrum Protect. Убедитесь, что у каждого сервера существует отдельное положение хранения, которым владеет и управляет данный сервер.

- Windows: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами
  Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.
- Windows: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов
  Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.

- Windows: Пример: оценка размера активного и архивного журналов для операций одновременной записи
  Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.
- Windows: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера
  Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.
- Windows: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности
  Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.
- Windows: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных
  Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.
- Windows: Пример: оценка размера активных и архивных журналов для операций дедупликации данных
  Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Windows: Пример: оценка размера активного и архивного журналов для основных операций сохранения данных клиентами

Основные операции сохранения данных клиентами включают в себя резервное копирование, архивирование и управление пространством. Пространство журналов должно быть достаточно большим, чтобы обрабатывать все выполняемые одновременно операции сохранения.

Чтобы определить размеры активных и архивных журналов для основных операций сохранения, выполняемых клиентами, используйте следующую формулу:

```
число клиентов  x  число файлов, сохраненных в течение каждой транзакции
  x  размер пространства журнала, необходимый для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Основные операции сохранения данных клиентами

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Элемент	Значения примера	Описание
Размер пространства журналов, необходимый для каждого файла	3053 байта	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	19,5 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 байт = 3,5 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`3,5 + 16 = 19,5 ГБ`

Архивный журнал: Рекомендуемый размер	58,5 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала.
		
		`3,5 x 3 = 10,5 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`10,5 + 48 = 58,5 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Windows: Пример: оценка размеров активных и неактивных журналов для клиентов, использующих несколько сеансов

Если для опции клиента RESOURCEUTILIZATION задано большее значение, чем по умолчанию, из-за одновременности выполнения увеличивается рабочая нагрузка на сервер.

Чтобы определить размеры активных и архивных журналов, когда клиенты используют несколько сеансов, примените следующую формулу:

```
число клиентов  x  число сеансов для каждого клиента  x  число файлов, сохраненных
  в течение каждой транзакции  x  объем памяти журнала, необходимой для каждого файла
```

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Несколько сеансов клиента

Элемент	Значения примера		Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	1000	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Возможных сеансов для каждого клиента	3	3	Параметр опции клиента RESOURCEUTILIZATION больше, чем значение по умолчанию. Каждый сеанс клиента запускает параллельно до трех сеансов.
Количество файлов, сохраняемых за каждую транзакцию	4096	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.
Размер пространства журналов, необходимый для каждого файла	3053	3053	Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	26,5 ГБ [1]	51 ГБ [1]	Следующие вычисления проведены для 300 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(300 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 10,5 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`10,5 + 16 = 26,5 ГБ`
			
			Следующие вычисления проведены для 1000 клиентов: Один гигабайт равен 1 073 741 824 байт.
			
			`(1000 клиентов x 3 сеанса на каждого клиента x 4096 сохраняемых за каждую транзакцию файлов x 3053 байта на каждый файл) ÷ 1 073 741 824 = 35 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`35 + 16 = 51 ГБ`

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	79,5 ГБ [1]	153 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
			`10,5 x 3 = 31,5 ГБ`
			`35 x 3 = 105 ГБ`
			Увеличим эти размеры на рекомендуемый начальный размер 48 ГБ:
			`31,5 + 48 = 79,5 ГБ`
			`105 + 48 = 153 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте ваш активный журнал и при необходимости настраивайте его размер.

Windows: Пример: оценка размера активного и архивного журналов для операций одновременной записи

Если операции резервного копирования клиентов используют пулы хранения, которые сконфигурированы для одновременной записи, увеличивается объем пространства журнала, требуемого для каждого файла.

Пространство журнала, требуемое для каждого файла, увеличивается примерно на 200 байт на каждый пул хранения копий, который используется для операции одновременной записи. В примере в следующей таблице данные сохраняются в двух пулах хранения копий в дополнение к первичному пулу хранения. Оценочный размер журнала увеличивается на 400 байт для каждого файла. Если использовать рекомендованное значение памяти журнала для каждого файла (3053 байта), полный объем составит 3453 байта.

Такое вычисление использовано в примере в следующей таблице.

Табл. 1. Одновременные операции записи

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Элемент	Значения примера	Описание
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байта на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 сохраняемых за каждую транзакцию файлов x 3453 байта на каждый файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендуемый размер	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить требования к размеру архивного журнала:
		
		`4 ГБ x 3 = 12 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`12 + 48 = 60 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Предлагаемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Windows: Пример: оценка размера активных и архивных журналов для основных операций сохранения данных клиентами и операций сервера

Перемещения данных в хранилище сервера, процессы идентификации для дедупликации, освобождение памяти и обработка устаревших данных могут происходить одновременно с операциями сохранения данных клиентами. Задачи администрирования, такие как административные команды и запросы SQL от клиентов администрирования, могут также выполняться одновременно с операциями сохранения данных клиентами. Операции сервера и административные задачи, выполняемые одновременно, могут увеличить требуемый объем памяти активного журнала.

Например, перемещение данных из дискового пула хранения с произвольным доступом (DISK) в дисковый пул хранения с последовательным доступом (FILE) использует примерно 110 байт памяти журнала на каждый перемещаемый файл. Допустим, например, что у вас есть 300 клиентов архивирования и резервного копирования, и каждый из них проводит резервное копирование 100 000 файлов каждую ночь. Файлы изначально хранятся в пуле хранения DISK, а затем переносятся в пул хранения FILE. Чтобы оценить объем памяти активного журнала, требуемой для этого перемещения данных, воспользуемся следующим вычислением. Число клиентов в формуле представляет собой максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время.

```
300 клиентов  x 100 000 файлов на каждого клиента  x  110 байт =  3,1 ГБ
```

Добавьте это значение к оценке размера активного журнала, полученной для основных операций сохранения данных клиентами.

Windows: Пример: оценка размера активных и архивных журналов в условиях сильной неоднородности

Проблемы с недостатком памяти для активного журнала могут возникнуть в том случае, если есть много быстро заканчивающихся транзакций и несколько транзакций, которым требуется гораздо больше времени для завершения. Типичная ситуация возникает, когда активны многие сеансы резервного копирования рабочих станций или файл-серверов и одновременно активны несколько сеансов резервного копирования очень больших баз данных. Если такая ситуация применима к вашей среде, вам может потребоваться увеличить размер памяти активного журнала, чтобы работа завершилась успешно.

Windows: Пример: Оценка размеров архивных журналов с полными резервными копиями базы данных

Сервер IBM Spectrum Protect удаляет ненужные файлы из архивного журнала только после полного резервного копирования базы данных. Следовательно, при оценке требуемой для архивного журнала памяти необходимо учитывать и периодичность полного резервного копирования базы данных.

Например, если полное резервное копирование базы данных производится раз в неделю, размер архивного журнала должен быть достаточным, чтобы содержать всю информацию за неделю в архивном журнале.

Различие в размерах архивного журнала для ежедневных и полных резервных копирований базы данных показано в примере в следующей таблице.

Табл. 1. Полное резервное копирование базы данных

Элемент	Значения примера	Описание
Максимальное число клиентских узлов, в которых одновременно выполняется резервное копирование, архивирование и перенос данных в любое время	300	Число клиентских узлов, в которых производится резервное копирование, архивирование и перенос данных каждую ночь.
Количество файлов, сохраняемых за каждую транзакцию	4096	Значение опции сервера TXNGROUPMAX по умолчанию - 4096.

Элемент	Значения примера	Описание
Размер пространства журналов, необходимый для каждого файла	3453 байта	3053 байт на каждый файл плюс 200 байт на каждый пул хранения копий. Значение 3053 байта для каждого файла в транзакции представляет количество байт в журнале, необходимое для резервного копирования файлов от клиента Windows, где длина имен файлов - от 12 до 120 байт. Это значение основывается на результатах тестов, выполненных в лабораторных условиях. Эти тесты включали в себя клиенты резервного копирования и архивирования, выполнявшие операции резервного копирования в дисковый пул хранения с произвольным доступом (DISK). Пулы DISK приводят к большему размеру журналов, чем пулы хранения последовательного доступа. Применяйте в расчетах значения, большие 3053 байт, если длина имен сохраняемых файлов - больше, чем от 12 до 120 байт.

Активный журнал: Рекомендуемый размер	20 ГБ [1]	Используйте следующую формулу для вычисления размера активного журнала. Один гигабайт равен 1 073 741 824 байт.
		
		`(300 клиентов x 4096 файлов на транзакцию x 3453 байт на файл) ÷ 1 073 741 824 байт = 4,0 ГБ`
		
		Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
		
		`4 + 16 = 20 ГБ`

Архивный журнал: Рекомендованный размер при ежедневном полном резервном копировании базы данных	60 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала:
		
		`4 ГБ x 3 = 12 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`12 + 48 = 60 ГБ`

Архивный журнал: Рекомендованный размер при еженедельном полном резервном копировании базы данных	132 ГБ [1]	Из-за требования возможности сохранения архивных журналов за три цикла резервного копирования базы данных сервера умножьте этот оценочный размер активного журнала на 3, чтобы оценить суммарные требования к размеру архивного журнала. Умножим этот результат на число дней между полными резервными копированиями базы данных:
		
		`(4 ГБ x 3 ) x 7 = 84 ГБ`
		
		Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
		
		`84 + 48 = 132 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, предлагаемый минимальный размер активного журнала - 16 ГБ. Рекомендуемый начальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 48 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 16 ГБ и 48 ГБ, используйте большие величины для оценки размера активного и архивного журнала.

Отслеживайте свои журналы и при необходимости настраивайте их размеры.

Windows: Пример: оценка размера активных и архивных журналов для операций дедупликации данных

Если используется дедупликация данных, необходимо рассмотреть ее влияние на требования к размеру пространства активных и архивных журналов.

Следующие факторы влияют на требования к размеру пространства активных и архивных журналов:

Объем дедуплицированных данных
: Влияние дедупликации данных на размер активного и архивного журналов зависит от процентной доли данных, которые могут использоваться для дедупликации. Если эта процентная доля данных для дедупликации относительно велика, потребуется больший объем пространства журналов.

Размер и количество экстентов
: Для каждого экстента, идентифицированного в процессе подготовки дедупликации, требуется примерно 1500 байт в пространстве активного журнала. Например, если при подготовке процесса дедупликации идентифицировано 250 тысяч экстентов, оценочный объем активного журнала составляет:

```
250 000 идентифицированных в каждом процессе экстентов x 1500 байт
 для каждого экстента = 358 МБ
```

Рассмотрим следующий сценарий: Триста клиентов архива резервных копий проводят каждую ночь до 100 тысяч операций резервного копирования файлов. Эти операции создают рабочую нагрузку в 30 миллионов файлов. Среднее количество экстентов для каждого файла - два. Следовательно, полное число экстентов - 60 миллионов, а для архивного журнала требуется 84 ГБ памяти:

```
60 000 000 экстентов x 1500 байт на каждый экстент = 84 ГБ
```

Процесс идентификации дубликатов оперирует с агрегатами файлов. Агрегат состоит из файлов, которые сохранены в данной транзакции, как задано опцией сервера TXNGROUPMAX. Предположим, что по умолчанию для опции сервера TXNGROUPMAX задано значение 4096. Если среднее число экстентов для каждого файла - два, общее число экстентов в каждом агрегате - 8192, а требуемая память активного журнала - 12 МБ:

```
8192 экстента в каждом агрегате x 1500 байт на каждый экстент =
   12 МБ
```

Время выполнения и число процессов идентификации дубликатов
: Время выполнения и число процессов идентификации дубликатов также влияют на размер активного журнала. Если использовать оцененный в предыдущем примере размер активного журнала (12 МБ), при параллельном выполнении десяти процессов идентификации дубликатов одновременная нагрузка активного журнала составит 120 МБ:

```
12 МБ на каждый процесс x 10 процессов = 120 МБ
```

Размер файла
: На размер активного журнала могут влиять также большие файлы, обрабатываемые для идентификации дубликатов. Допустим, например, что клиент резервного копирования и архивирования производит резервную копию около 80 гигабайтов (снимок файловой системы). В этом объекте может содержаться большое число дублированных экстентов, например, если проводилось инкрементное резервное копирование включенных в файловую систему файлов. Допустим, например, что снимок файловой системы содержит 1,2 миллиона дублированных экстентов. Эти 1,2 миллиона экстентов в таком большом файле представляют единственную транзакцию для процесса идентификации дубликатов. Требуемая для этого единственного объекта полная память активного журнала составляет 1,7 гигабайтов:

```
1 200 000 экстентов x 1500 байт на каждый экстент = 1,7 ГБ
```

Если одновременно с процессом идентификации дубликатов для этого большого объекта будет происходит аналогичный, но меньший по объему процесс, активному журналу может не хватить памяти. Допустим, например, что пул хранения включен для дедупликации. В пуле хранения содержится смесь данных, в том числе мелкие файлы с размером от 10 КБ до нескольких сотен КБ. В пуле хранения есть также несколько больших объектов, содержащих основную процентную долю дублированных экстентов.

Чтобы принять во внимание не только требования к объему памяти, но и затраты времени и продолжительность одновременных транзакций, увеличьте оцененный размер активного журнала примерно вдвое. Допустим, например, что ваша оценка дает для требуемого объема памяти значение 25 ГБ (23,3 ГБ + 1,7 ГБ на дедупликацию

большого объекта). Если процессы дедупликации выполняются одновременно, рекомендуемый размер активного журнала составит 50 ГБ. Предлагаемый размер архивного журнала - 150 ГБ.

Примеры в следующих таблицах показывают результаты расчетов для активных и архивных журналов. В примере первой таблицы использован средний размер экстента 700 КБ. Во втором примере (вторая таблица) средний размер экстента - 256 КБ. Как видно, меньший средний размер дубликата экстента (256 КБ) приводит к большему оцененному размеру активного журнала. Для исключения или минимизации проблем функционирования сервера используйте значение 256 КБ для оценки размера активного журнала в вашей производственной среде.

Табл. 1. Средний размер дубликата экстента - 700 КБ

Элемент	**Значения примера**		**Описание**
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	700 КБ	700 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.
Экстенты для данного файла	1 198 372 бит	6 135 667 бит	При использовании среднего размера экстентов (700 КБ) эта оценка дает среднее число экстентов для данного объекта. Для объекта размером 800 ГБ была использована следующая формула: `(800 ГБ ÷ 700 КБ) = 1 198 372 бит` Аналогичные вычисления для объекта размером 4 ТБ: `(4 ТБ ÷ 700 КБ) = 6 135 667`
Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	1,7 ГБ	8,6 ГБ	Оценка размера активного журнала, требуемого для этой транзакции.

Элемент	Значения примера		Описание

Активный журнал: Рекомендуемый общий размер	66 ГБ [1]	79,8 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 1,7 ГБ) x 2 = 50 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`50 + 16 = 66 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 8,6 ГБ) x 2 = 63,8 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`63,8 + 16 = 79,8 ГБ`

Архивный журнал: Рекомендуемый размер	198 ГБ [1]	239,4 ГБ [1]	Увеличьте оцененный размер активного журнала втрое.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`50 ГБ x 3 = 150 ГБ`
			
			Увеличим этот размер на рекомендуемый начальный размер 48 ГБ:
			
			`150 + 48 = 198 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`63,8 ГБ x 3 = 191,4 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`191,4 + 48 = 239,4 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.			

Табл. 2. Средний размер дубликата экстента - 256 КБ

Элемент	Значения примера	Описание

Элемент	Значения примера		Описание
Размер наибольшего единичного объекта для дедупликации	800 ГБ	4 ТБ	Детализация обработки для дедупликации - на уровне файлов. Поэтому наибольший единичный файл для дедупликации представляет собой наибольшую транзакцию и соответствующую большую нагрузку для активного и архивного журналов.
Средний размер экстентов	256 КБ	256 КБ	Алгоритмы дедупликации используют метод переменных блоков. Не у всех дедуплицированных экстентов данного файла одинаковый размер, поэтому для оценки используется средний размер экстентов.

Экстенты для данного файла	3 276 800 бит	16 777 216 бит	При использовании среднего размера экстентов эта оценка дает среднее число экстентов для данного объекта.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(800 ГБ ÷ 256 КБ) = 3 276 800 бит`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(4 ТБ ÷ 256 КБ) = 16 777 216 бит`

Активный журнал: Оценочный размер, требуемый для дедупликации единичного большого объекта во время единичного процесса идентификации дубликатов	4,5 ГБ	23,4 ГБ	Оценочный размер памяти активного журнала, требуемой для этой транзакции.

Активный журнал: Рекомендуемый общий размер	71,6 ГБ [1]	109,4 ГБ [1]	Принимая во внимание другие аспекты рабочей нагрузки сервера в дополнение к дедупликации, увеличьте существующую оценку вдвое. В этих примерах требуемый для дедупликации единичного большого объекта размер памяти активного журнала рассматривается с учетом ранее полученной оценки требуемого размера активного журнала.
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 800 ГБ:
			
			`(23,3 ГБ + 4,5 ГБ) x 2 = 55,6 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`55,6 + 16 = 71,6 ГБ`
			
			В следующих вычислениях рассматривается несколько транзакций и объект размером 4 ТБ:
			
			`(23,3 ГБ + 23,4 ГБ) x 2 = 93,4 ГБ`
			
			Увеличьте этот размер на рекомендуемый начальный размер в 16 ГБ:
			
			`93,4 + 16 = 109,4 ГБ`

Элемент	Значения примера		Описание

Архивный журнал: Рекомендуемый размер	214,8 ГБ [1]	328,2 ГБ [1]	Троекратный размер оценки активного журнала.
			
			Следующие вычисления проведены для объекта размером 800 ГБ:
			
			`55,6 ГБ x 3 = 166,8 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`166,8 + 48 = 214,8 ГБ`
			
			Следующие вычисления проведены для объекта размером 4 ТБ:
			
			`93,4 ГБ x 3 = 280,2 ГБ`
			
			Учтем увеличение этого размера за счет оцененного начального размера в 48 ГБ:
			
			`280,2 + 48 = 328,2 ГБ`

[1] Значения примера в этой таблице используются только, чтобы показать, как вычисляются размеры активных журналов и архивных журналов. В производственной среде, где не используется дедупликация, рекомендуемый минимальный размер активного журнала - 32 ГБ. Рекомендуемый минимальный размер архивного журнала в производственной среде, где не используется дедупликация, составляет 96 ГБ. Если при подстановке в приведенные оценки значений для вашей среды получатся результаты, превышающие 32 ГБ и 96 ГБ, используйте большие величины для оценки размера активного и архивного журнала. Отслеживайте свои журналы и при необходимости настраивайте их размеры.			

Windows: Пространство зеркальной копии активного журнала

Можно использовать зеркальную копию активного журнала, если не удастся прочитать файлы активного журнала. Может существовать только одна зеркальная копия активного журнала.

Создание зеркальной копии журнала - рекомендуемая опция. Если вы увеличите размер активного журнала, размер зеркальной копии журнала увеличится автоматически. Зеркальное копирование журнала может отрицательно сказаться на производительности, так как при зеркальном копировании потребуется удвоенный объем операций ввода-вывода. Дополнительное пространство, которое требуется для зеркальной копии журнала - это еще один фактор, который следует учесть, при принятии решения относительно создания зеркальной копии журнала.

Если каталог зеркальной копии журнала переполняется, сервер записывает сообщения об ошибке в активный журнал и в файл db2diag.log. Работа сервера продолжится.

Windows: Пространство резервного архивного журнала

Резервный архивный журнал используется сервером, если в каталоге архивного журнала не хватает места.

Задав каталог резервного архивного журнала, можно предотвратить ошибки, которые могут происходить при нехватке места в каталоге архивного журнала. Если переполнятся и каталог архивного журнала, и диск или файловая система, где находится каталог резервного архивного журнала, данные останутся в каталоге активного журнала. Это условие может привести к остановке сервера в связи с переполнением активного журнала.

Windows: Мониторинг использования пространства для базы данных и журналов восстановления

Для определения размера используемого и доступного пространства активного журнала введите команду QUERY LOG. Для отслеживания использования пространства базой данных и журналами восстановления можно проверить также записи в журнале операций.

Активный журнал

Если объем доступного пространства активного журнала недостаточен, в журнале операций появятся следующие записи:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Сервер IBM Spectrum Protect начинает полное резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
: Это сообщение выводится, когда объем пространства активного журнала превышает максимальный заданный размер. Надо вручную выполнить резервное копирование базы данных.

  Чтобы изменить максимальный размер журнала, остановите сервер. Откройте файл dsmserv.opt и задайте новое значение для опции ACTIVELOGSIZE. По завершении операции перезапустите сервер.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
: Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Если должно будет начаться хотя бы одно полное резервное копирование базы данных, сервер IBM Spectrum Protect начнет инкрементное резервное копирование базы данных. В противном случае сервер начнет полное резервное копирование базы данных.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
: Отношение размера используемого пространства активного журнала к доступному размеру пространства активного журнала превышает порог использования журнала. Надо вручную выполнить резервное копирование базы данных.

Архивный журнал

Если объем доступного пространства архивного журнала недостаточен, в журнале операций появится следующая запись:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
: Отношение размера используемого пространства архивного журнала к доступному размеру пространства архивного журнала превышает порог использования журнала. Сервер IBM Spectrum Protect начинает автоматическое полное резервное копирование базы данных.

Database

Если объем доступного пространства для операций базы данных недостаточен, в журнале операций появятся следующие сообщения:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
: Используемое пространство базы данных превышает порог использования пространства базы данных. Чтобы увеличить размер пространства для базы данных, используйте команду EXTEND DBSPACE, команду EXTEND DBSPACE или утилиту DSMSERV FORMAT с параметром DBDIR.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
: Размер доступного пространства в каталоге, где расположены серверные файлы базы данных, меньше 1 ГБ.

  Когда сервер IBM Spectrum Protect создается при помощи утилиты DSMSERV FORMAT или мастера по конфигурированию, одновременно создаются база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных. Указанный в этом сообщении каталог обозначает положение информации о базе данных, используемой менеджером баз данных. Если в этом каталоге нет доступного пространства, сервер больше не может функционировать.

  Необходимо добавить пространство к файловой системе или обеспечить доступное пространство в файловой системе или на диске.

Windows: Удаление файлов отката установки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, чтобы высвободить пространство в каталоге совместно используемого ресурса. Например, файлы, которые, возможно, требовались для операции отката, это те файлы, которые можно удалить.

Об этой задаче

Чтобы удалить файлы, которые больше не нужны, используйте либо графический мастер установки, либо командную строку в режиме консоли.

- Windows: Удаление файлов отката установки с использованием графического мастера
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.
- Windows: Удаление файлов отката установки с использованием командной строки
  Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Windows: Удаление файлов отката установки с использованием графического мастера

Можно удалить определенные файлы установки, сохраненные во время процесса установки, используя пользовательский интерфейс IBM® Installation Manager.

Процедура

1. Откройте IBM Installation Manager.
2. Щелкните по Файл > Предпочтения.
3. Выберите Файлы для отката.
4. Щелкните по Удалить сохраненные файлы и нажмите на OK.

Windows: Удаление файлов отката установки с использованием командной строки

Можно удалить определенные файлы установки, сохраненные во время процесса установки, при помощи командной строки.

Процедура

1. В каталоге, в котором установлен IBM® Installation Manager, перейдите в следующий подкаталог:
   -  Операционные системы Windowseclipse\tools

   Например:

   -  Операционные системы WindowsC:\Program Files\IBM\Installation Manager\eclipse\tools
2. В каталоге tools введите следующую команду, чтобы запустить командную строку IBM Installation Manager:
   -  Операционные системы Windows`imcl.exe -c`
3. Введите `I`, чтобы выбрать Предпочтения.
4. Введите `3`, чтобы выбрать Файлы для отката.
5. Введите `D`, чтобы удалить файлы для отката.
6. Введите `A`, чтобы применить изменения и вернуться в меню предпочтений.
7. Введите `C`, чтобы выйти из Меню предпочтений.
8. Введите `X`, чтобы закрыть Installation Manager.

Windows: Практические рекомендации по именованию сервера

Используйте эти описания для справки при установке или обновлении сервера IBM Spectrum Protect.

ID пользователя экземпляра

ID пользователя экземпляра служит основой для других имен, связанных с экземпляром сервера. ID пользователя экземпляра также называют владельцем экземпляра.

Например: tsminst1

ID пользователя экземпляра - это ID пользователя, у которого должны быть полномочия владельца или доступ с правом на чтение/запись для всех каталогов, которые вы создаете для базы данных и журнала восстановления. Обычная практика работы сервера - его запуск от имени ID пользователя экземпляра. У этого ID пользователя должно быть право чтения и записи в каталоги, используемые для всех классов устройств FILE.

 Операционные системы Windows

Имя экземпляра базы данных

Имя экземпляра базы данных - эти имя экземпляра сервера в том виде, в каком оно представлено в реестре.

Например: Server1

 Операционные системы Windows

Каталог экземпляра

Каталог экземпляра - это каталог, содержащий связанные с экземпляром сервера файлы (файл опций сервера и другие специфичные для сервера файлы). У этого каталога может быть любое имя по вашему выбору. Чтобы этот каталог было проще распознать, используйте имя, связывающее каталог с именем экземпляра.

Можно использовать имя, содержащее имя экземпляра сервера в том виде, в каком оно представлено (или появится) в реестре. По умолчанию, имена экземпляров сервера имеют вид Server*x*.

Например: C:\tsm\server1

В каталоге экземпляра хранятся следующие файлы для экземпляра сервера:

- Файл серверных опций, dsmserv.opt
- Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
- Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
- Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
- Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.
- Обработчики пользователя
- Выходная информация трассировки (если не задано полное имя)

Имя базы данных

Именем базы данных для каждого экземпляра сервера всегда является TSMDB1. Это имя нельзя изменить.

Имя сервера

Имя сервера - это внутреннее имя для IBM Spectrum Protect, и оно используется для выполнения операций, включающих в себя взаимодействия между несколькими серверами IBM Spectrum Protect. В качестве примера можно привести взаимодействие сервера с сервером и совместное использование библиотеки.

 Операционные системы WindowsИмя сервера также используется при добавлении сервера в Центр операций, чтобы им можно было управлять с использованием этого интерфейса. Используйте для каждого сервера уникальное имя. Чтобы имя было проще распознать в Центре операций или в выходной информации команды QUERY SERVER, используйте имя, отражающее положение или назначение сервера. Не изменяйте имя сервера IBM Spectrum Protect после того, как он сконфигурирован как хаб или подчиненный сервер.

Если вы используете мастер, рекомендуемым именем по умолчанию будет имя хоста компьютера, который вы используете. Можно использовать другое имя, которое будет иметь смысл в вашей среде. Если у вас в системе более одного сервера и вы используете мастер, вы сможете использовать имя по умолчанию только для одного из серверов. Для каждого сервера нужно ввести уникальное имя.

 Операционные системы WindowsНапример:

- `TUCSON_SERVER1`
- `TUCSON_SERVER2`

Каталоги для пространства базы данных и журнала восстановления

Каталогам можно присваивать имена в соответствии с принятой у вас практикой. Чтобы было проще распознавать каталоги, используйте имена, связывающие каталоги с экземпляром сервера.

Например, в случае архивного журнала:

-  Операционные системы Windowsf:\server1\archlog

Windows: Каталоги установки

К каталогам установки сервера IBM Spectrum Protect относятся каталог сервера, каталог DB2, каталог устройств, каталог языка и другие каталоги. В каждом из них содержится несколько дополнительных каталогов.

(/opt/tivoli/tsm/server/bin) - это каталог по умолчанию, содержащий код сервера и файлы лицензии.

Структура каталогов продукта DB2, устанавливаемого в ходе установки сервера IBM Spectrum Protect, соответствует тому, что задокументировано в источниках информации по DB2. Защищайте эти каталоги и файлы так же, как вы защищаете каталоги сервера. Каталог по умолчанию - /opt/tivoli/tsm/db2.

Можно использовать следующий языки: английский (США), испанский, итальянский, китайский Big5, китайский GBK, китайский традиционный, китайский упрощенный, корейский, немецкий, португальский (Бразилия), русский, французский и японский.

Windows: Установка компонентов сервера

Чтобы установить компоненты сервера версии 8.1.5, можно использовать мастер установки, командную строку в режиме консоли или режим без вывода сообщений.

Об этой задаче

При использовании программы установки IBM Spectrum Protect можно установить следующие компоненты:

- сервер (server)
  Совет: База данных (DB2), Global Security Kit (GSKit) и IBM® Java™ Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- языки сервера
- лицензия
- устройства
- IBM Spectrum Protect for SAN
- Центр операций

 Операционные системы WindowsДля установки сервера версии 8.1.5 надо выделить примерно 15 - 30 минут.

- Windows: Получение пакета установки
  Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM (например, Passport Advantage или IBM Fix Central).
- Windows: Установка IBM Spectrum Protect при помощи мастера установки
  Сервер можно установить при помощи графического мастера IBM Installation Manager.
- Windows: Установка IBM Spectrum Protect в режиме консоли
  IBM Spectrum Protect можно установить из командной строки в режиме консоли.
- Windows: Установка IBM Spectrum Protect в режиме без вывода сообщений
  Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.
- Windows: Установка языковых пакетов сервера
  Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Windows: Получение пакета установки

Пакет установки IBM Spectrum Protect можно получить с сайта скачивания IBM® (например, Passport Advantage или IBM Fix Central).

Процедура

1. Загрузите нужный файл пакета с одного из следующих веб-сайтов.
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.
   - Самую свежую информацию, обновления и исправления обслуживания смотрите по адресу: Портал поддержки IBM.
2. Если вы скачали пакет с сайта скачивания IBM, то сделайте следующее:
    Операционные системы Windows
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к свободному месту можно увидеть в документе по скачиванию:
      - IBM Spectrum Protect техническое замечание 4042944
      - IBM Spectrum Protect Extended Edition техническое замечание 4042945
      - IBM Spectrum Protect for Data Retention техническое замечание 4042946

   b. Перейдите в каталог, куда вы поместили исполняемый файл.
   Важное замечание: В следующем шаге файлы извлекаются в текущий каталог. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.

   c. Чтобы извлечь файлы программы установки, либо дважды щелкните по выполняемому файлу, либо введите указанную ниже команду в командной строке. Файлы извлекаются в текущий каталог.

   ```
   имя_пакета.exe
   ```

   где *имя_пакета* выглядит, как в следующем примере: *8.1.x.000*-IBM-SPSRV-WindowsX64.exe

3. Выберите один из следующих способов установки IBM Spectrum Protect:
   - Windows: Установка IBM Spectrum Protect при помощи мастера установки
   - Windows: Установка IBM Spectrum Protect в режиме консоли
   - Windows: Установка IBM Spectrum Protect в режиме без вывода сообщений
4. После установки IBM Spectrum Protect и до настройки этого продукта в соответствии с вашими требованиями посетите следующий веб-сайт: Портал поддержки IBM. Щелкните по Support and downloads (Поддержка и материалы для скачивания) и примените все требуемые исправления.

Windows: Установка IBM Spectrum Protect при помощи мастера установки

Сервер можно установить при помощи графического мастера IBM® Installation Manager.

Прежде чем начать

Перед запуском установки сделайте следующее:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
-  Операционные системы WindowsУбедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки, введя следующую команду:  Операционные системы Windows `install.bat`  Операционные системы WindowsМожно также дважды щелкнуть по файлу install.bat (в каталоге, куда были распакованы файлы установки).

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM Installation Manager.

  Вы можете просмотреть файлы журнала установки, выбрав Файл > Просмотреть журнал в инструменте Installation Manager. Чтобы выполнить сбор этих файлов журнала, выберите Справка > Экспорт данных для анализа проблем в инструменте Installation Manager.

- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.

-  Операционные системы WindowsПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.
-  Операционные системы WindowsЕсли в Windows доступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, используйте этот собственный драйвер устройств. Если в Windows недоступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, установите драйвер устройства IBM Spectrum Protect при помощи команды `dpinst.exe /a`. Файл `dpinst.exe` находится в каталоге драйверов устройств. Каталог по умолчанию - C:\Program Files\Tivoli\TSM\device\drivers.

Windows: Установка IBM Spectrum Protect в режиме консоли

IBM Spectrum Protect можно установить из командной строки в режиме консоли.

Прежде чем начать

Перед запуском установки сделайте следующее:

- Убедитесь, что для операционной системы задан нужный язык. По умолчанию язык операционной системы - это язык мастера по установке.
-  Операционные системы WindowsУбедитесь, что у ID пользователя, который вы планируете использовать для установки, есть полномочия локального администратора.

Процедура

Установите IBM Spectrum Protect, используя следующий метод:

Опция	Описание
Установка программы из скачанного пакета:	a. Перейдите в каталог, в который вы скачали пакет.. b. Запустите мастер установки в консольном режиме, введя следующую команду:  Операционные системы Windows `install.bat -c` Необязательно: Сгенерируйте файл ответов в ходе установки в режиме консоли. Укажите опции установки в режиме консоли и на панели Сводка укажите `G`, чтобы сгенерировать ответы.

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  - Операционные системы WindowsC:\ProgramData\IBM\Installation Manager\logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
- Операционные системы WindowsПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.
- Операционные системы WindowsЕсли в Windows доступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, используйте этот собственный драйвер устройств. Если в Windows недоступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, установите драйвер устройства IBM Spectrum Protect при помощи команды `dpinst.exe /a`. Файл `dpinst.exe` находится в каталоге драйверов устройств. Каталог по умолчанию - C:\Program Files\Tivoli\TSM\device\drivers.

Windows: Установка IBM Spectrum Protect в режиме без вывода сообщений

Сервер можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге input в том месте, куда был распакован пакет установки:

install_response_sample.xml
: Используйте этот файл для установки компонентов IBM Spectrum Protect.

update_response_sample.xml
: Используйте этот файл для обновления компонентов IBM Spectrum Protect.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов. Вы можете изменить пример файла ответов или создать свой собственный.
2. Если вы устанавливаете сервер и компонент Центр операций в режиме без вывода сообщений, создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.
   Если вы используете файл install_response_sample.xml, добавьте пароль в следующую строку в файле, где *пароль* - это пароль:

   ```
   <variable name='ssl.password' value='пароль' />
   ```

   Дополнительную информацию об этом пароле смотрите в разделе Контрольный список установки.
   Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл update_response_sample.xml для обновления компонента Центр операций.
3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:
   - Операционные системы Windows

     ```
     install.bat -s -input файл_ответов -acceptLicense
     ```

Дальнейшие действия

- Если в процессе установки возникают ошибки, то они записываются в файлы журнала, которые хранятся в каталоге журналов IBM® Installation Manager, например:
  - Операционные системы WindowsC:\ProgramData\IBM\Installation Manager\logs
- После установки сервера и компонентов и до настройки этого продукта в соответствии с вашими требованиями посетите сайт Портал поддержки IBM. Щелкните по Downloads (fixes and PTFs) (Скачивание: исправления и PTF) и примените все требуемые исправления.
- Операционные системы WindowsПосле установки нового сервера ознакомьтесь с разделом Первые шаги после установки IBM Spectrum Protect, чтобы узнать, как сконфигурировать сервер.
- Операционные системы WindowsЕсли в Windows доступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, используйте этот собственный драйвер устройств. Если в Windows недоступен собственный драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, установите драйвер устройства IBM Spectrum Protect при помощи команды `dpinst.exe /a`. Файл `dpinst.exe` находится в каталоге драйверов устройств. Каталог по умолчанию - C:\Program Files\Tivoli\TSM\device\drivers.

Операционные системы Windows

Windows: Установка языковых пакетов сервера

Переводы для сервера позволяют серверу показывать сообщения и справку на языках, отличных от английского (США). Такие переводы позволяют также использовать региональные стандарты представления дат, времени и чисел.

Прежде чем начать

Инструкции по установке пакетов поддержки национальных языков для агента хранения смотрите в документе Конфигурация пакета поддержки национальных языков для агентов хранения.

- Windows: Локали языка сервера
  Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.
- Windows: Конфигурирование языкового пакета
  После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.
- Windows: Обновление языкового пакета
  Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

Windows: Локали языка сервера

Либо используйте опцию языкового пакета по умолчанию, либо выберите другой языковой пакет для вывода сообщений и справки сервера.

Операционные системы WindowsЭтот языковый пакет автоматически устанавливается для следующей языковой опции по умолчанию для сообщений и справки сервера: LANGUAGE AMENG.

Для прочих языков и локалей установите языковой пакет, нужный для вашей установки.
Можно использовать следующие языки:
Операционные системы Windows

Табл. 1. Языки сервера для Windows

Язык	**Значение опции LANGUAGE**
Китайский упрощенный	chs
Китайский традиционный	cht
Английский	ameng
Французский	fra
Немецкий	deu
Итальянский	ita
Japanese (Shift-JIS)	jpn

Язык	Значение опции LANGUAGE
Корейский	kor
Бразильский португальский	ptb
Русский	rus
Испанский	esp

 Операционные системы WindowsОграничение: При использовании Центр операций некоторые символы могут выводиться неправильно, если язык веб-браузера не совпадает с языком сервера. При появлении этой неполадки следует сконфигурировать в браузере использование того же языка, что и на сервере.

Windows: Конфигурирование языкового пакета

После конфигурирования языкового пакета сообщения и справки выводятся на сервере на языке, отличном от английского (США). Пакеты установки входят в комплект поставки программного обеспечения IBM Spectrum Protect.

Об этой задаче

 Операционные системы WindowsДля опции LANGUAGE в файле опций сервера задайте имя локали, которую нужно использовать. Например, для использования локали `rus` задайте для опции LANGUAGE значение `rus`. Смотрите раздел Windows: Локали языка сервера.

Если локаль успешно инициализирована, то с ее помощью форматируется дата, время и представление чисел для сервера. Если локаль не инициализируется успешно, сервер будет использовать файлы сообщений на английском языке (США), а также формат дат времени и чисел для языка системы 'Английский (США)'.

Windows: Обновление языкового пакета

Вы можете изменить или обновить языковой пакет при помощи IBM® Installation Manager.

Об этой задаче

Внутри одного и того же экземпляра IBM Spectrum Protect можно установить другой языковой пакет.

- Для установки другого языкового пакета используйте функцию Изменить программы IBM Installation Manager.
- Для обновления языковых пакетов до новых версий используйте функцию Обновить программы IBM Installation Manager.

Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* являются синонимами.

Windows: Первые шаги после установки IBM Spectrum Protect

После установки версии 8.1.5 подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ для конфигурирования экземпляра IBM Spectrum Protect.

Об этой задаче

1. Создайте каталоги и ID пользователя для экземпляра сервера. Смотрите раздел Windows: Создание ID пользователя и каталогов для экземпляра сервера.
2. Сконфигурируйте экземпляр сервера. Выберите одну из следующих опций.
   - Воспользуйтесь мастером по конфигурированию - это рекомендуемый способ. Смотрите раздел Windows: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования.
   - Сконфигурируйте вручную новый экземпляр. Смотрите раздел Windows: Конфигурирование экземпляра сервера вручную. При конфигурировании вручную выполните описанные ниже шаги.
     a. Сконфигурируйте каталоги и создайте экземпляр IBM Spectrum Protect. Смотрите раздел Windows: Создание экземпляра сервера.
     b. Создайте новый файл серверных опций, скопировав пример файла, чтобы сконфигурировать связь между сервером и клиентами. Смотрите раздел Операционные системы WindowsWindows:

Конфигурирование связи между сервером и клиентом.
   c. Введите команду DSMSERV FORMAT, чтобы сформатировать базу данных. Смотрите раздел Windows: Форматирование базы данных и журнала.
   d. Сконфигурируйте систему для резервного копирования базы данных. Смотрите раздел Windows: Подготовка менеджера базы данных к резервному копированию базы данных.
3. Сконфигурируйте опции, чтобы задать, когда запускать реорганизацию базы данных. Смотрите раздел Windows: Опции конфигурирования сервера для обслуживания сервера баз данных.
4. Запустите экземпляр сервера, если он еще не запущен.
   -  Операционные системы WindowsСмотрите раздел Windows: Запуск экземпляра сервера в системах Windows.
5. Зарегистрируйте свою лицензию. Смотрите раздел Windows: Регистрация лицензий.
6. Подготовьте систему для резервного копирования базы данных. Смотрите раздел Windows: Подготовка сервера к операциям резервного копирования базы данных.
7. Наблюдайте сервер. Смотрите раздел Windows: Мониторинг сервера.

- Windows: Создание ID пользователя и каталогов для экземпляра сервера
  Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.
- Windows: Конфигурирование сервера IBM Spectrum Protect
  После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.
- Windows: Опции конфигурирования сервера для обслуживания сервера баз данных
  Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.
-  Операционные системы WindowsWindows: Запуск экземпляра сервера в системах Windows
  В производственной среде предпочтительным методом запуска сервера является запуск его как службы Windows. В среде, где вы производите переконфигурирование или тестирование либо выполняете задачи по обслуживанию, запускайте сервер в приоритетном режиме или используйте режим обслуживания.
- Windows: Остановка сервера
  При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.
- Windows: Регистрация лицензий
  Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.
- Windows: Подготовка сервера к операциям резервного копирования базы данных
  Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.
- Windows: Запуск нескольких экземпляров серверов на одном компьютере
  Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.
- Windows: Мониторинг сервера
  Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Windows: Создание ID пользователя и каталогов для экземпляра сервера

Создайте ID пользователя для экземпляра сервера IBM Spectrum Protect и каталоги, которые нужны экземпляру сервера для базы данных и журналов восстановления.

Прежде чем начать

Прежде чем выполнять данную задачу, ознакомьтесь с информацией о планировании пространства для сервера. Смотрите раздел Windows: Контрольные списки для планирования сведений о сервере.

Процедура

1. Создайте ID пользователя, который станет владельцем экземпляра сервера. Вы будете использовать этот ID пользователя при создании экземпляра сервера в одном из последующих шагов.

   Операционные системы Windows
   Операционные системы WindowsСоздайте ID пользователя, который станет владельцем экземпляра сервера IBM Spectrum Protect. ID пользователя может являться владельцем нескольких экземпляров сервера IBM Spectrum Protect. Укажите учетную запись пользователя, который будет владельцем экземпляра сервера.

   Если сервер запускается как служба Windows, нужно указать учетную запись, под которой будет входить в систему эта служба. У этой учетной записи пользователя должны быть полномочия администратора системы. Одна учетная запись пользователя может являться владельцем нескольких экземпляров сервера.

   Если в системе несколько серверов и вы хотите запускать каждый сервер от имени отдельной учетной записи пользователя, создайте в этом шаге новую учетную запись пользователя.

   Создайте ID пользователя.
   Ограничение: ID пользователя должен соответствовать следующим правилам:

   В ID пользователя можно использовать буквы нижнего регистра (a-z), цифры (0-9) и символ подчеркивания (_). ID пользователя не должен содержать более 30 символов и не должен начинаться с *ibm*, *sql*, *sys* или с цифры. В качестве ID пользователя или имени группы нельзя использовать *user*, *admin*, *guest*, *public*, *local* или какое-либо зарезервированное слово SQL.

   a. Чтобы создать ID пользователя, введите следующую команду операционной системы:

      ```
      net user ID_пользователя * /add
      ```

      Вам предложат создать и подтвердить пароль для нового ID пользователя.
   b. Введите указанные ниже команды операционной системы, чтобы добавить новый ID пользователя в группы администраторов:

      ```
      net localgroup Administrators ID_пользователя /add
      net localgroup DB2ADMNS ID_пользователя /add
      ```

2. Создайте каталоги, необходимые серверу.
   Операционные системы WindowsСоздайте пустые каталоги для каждого элемента в таблице и убедитесь, что у созданного ID пользователя есть разрешения 'чтение/запись' для каталогов. База данных, архивный журнал и активный журнал должны располагаться в разных физических томах.

Элемент	**Примеры команд для создания каталогов**	**Ваши каталоги**
Каталог экземпляра для сервера, представляющий собой каталог с файлами, связанными именно с данным экземпляром сервера (файл серверных опций и другие файлы, связанные с сервером)	`mkdir d:\tsm\server1`	

Каталоги базы данных	`mkdir d:\tsm\db001`
	`mkdir e:\tsm\db002`
	`mkdir f:\tsm\db003`
	`mkdir g:\tsm\db004`	

Каталог активного журнала	`mkdir h:\tsm\log`	
Каталог архивного журнала	`mkdir i:\tsm\archlog`	
Необязательно: Каталог для зеркальной копии активного журнала	`mkdir j:\tsm\logmirror`	
Необязательно: Каталог вторичного архивного журнала (каталог для резервного архивного журнала)	`mkdir k:\tsm\archlogfailover`	

При первоначальном создании сервера при помощи утилиты DSMSERV FORMAT или мастера конфигурирования создается база данных сервера и журнал восстановления. Кроме того, создаются файлы для хранения информации о базе данных, используемой менеджером базы данных.

3. Завершите сеанс для нового ID пользователя.

Windows: Конфигурирование сервера IBM Spectrum Protect

После того как вы установите сервер и подготовитесь к конфигурированию, сконфигурируйте экземпляр сервера.

Об этой задаче

Сконфигурируйте экземпляр сервера IBM Spectrum Protect, выбрав один из следующих вариантов:

- Windows: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования
  Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.
- Windows: Конфигурирование экземпляра сервера вручную
  После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

Windows: Конфигурирование IBM Spectrum Protect при помощи мастера конфигурирования

Мастер обеспечивает подход к конфигурированию сервера на основе набора шагов. Используя графический интерфейс пользователя, вы сможете обойти ряд шагов по конфигурированию, которые сложно выполнить вручную. Запустите мастер в системе, в которой вы установили программу сервера IBM Spectrum Protect.

Прежде чем начать

Прежде чем использовать мастер конфигурирования, нужно выполнить все предыдущие шаги для подготовки к конфигурированию. В число этих шагов входят установка IBM Spectrum Protect, создание каталогов базы данных и журналов и создание каталогов и ID пользователя для экземпляра сервера.
 Операционные системы Windows

Об этой задаче

Процедура

1. Убедитесь, что выполнены следующие требования:
   - Резервную копию следующих файлов нужно сохранить в безопасном и защищенном месте:
     - Файлы главного ключа шифрования (`dsmkeydb.*`)
     - Сертификат сервера и файлы секретных ключей (`cert.*`)

    Операционные системы Windows
   - Запустите службу удаленного реестра:
     a. Выберите Пуск > Администрирование > Службы.
     b. В окне Службы выберите службу Удаленный реестр, если она еще не запущена, и нажмите на Пуск.
   - Убедитесь, что следующие порты не заблокированы брандмауэром: 137, 139 и 445. Сделайте следующее:
     a. Щелкните по Запуск > Панель управления > Брандмауэр Windows.
     b. Выберите Дополнительные параметры.
     c. Выберите Входные правила в левой панели.
     d. Выберите Новое правило в правой панели:
     e. Создайте правило порта для портов TCP 137, 139 и 445 для разрешения соединений для доменных и частных сетей.
   - Сконфигурируйте Управление учетными записями пользователей:

     Получите доступ ко всем трем параметрам конфигурации управления учетными записями пользователей, получив сначала доступ к опциям Локальная безопасность политики безопасности. Сделайте следующее:

a. Включите встроенную учетную запись Администратора:
   - Выберите Учетные записи: Состояние учетной записи администратора.
   - Выберите Включить и щелкните по OK.

b. Выключите Управление учетными записями пользователей для всех администраторов Windows.
   - Выберите Управление учетной записью пользователя: Запускать всех администраторов в режиме Утверждать администраторов.
   - Выберите Выключить и щелкните по OK.

c. Выключите Управление учетными записями пользователей для встроенной учетной записи администратора:
   - Выберите Управление учетной записью пользователя: Режим Утверждать администраторов для встроенной учетной записи Администратор.
   - Выберите Выключить и щелкните по OK.

2. Запустите локальную версию мастера:
   - Операционные системы WindowsЩелкните по Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования. Можно также дважды щелкнуть по программе `dsmicfgx.exe`, находящейся в каталоге *каталог_установки*\server. Каталог по умолчанию - C:\Program Files\Tivoli\TSM.

   Завершите конфигурирование, следуя инструкциям. Мастер можно останавливать и перезапускать, но сервер не будет работать, пока не будет выполнена вся процедура конфигурирования.

- Операционные системы WindowsWindows: Конфигурирование протокола REXEC (Remote Execution Protocol) в Windows
  Сконфигурируйте удаленный доступ при помощи описанных в этом разделе процедур.

Windows: Конфигурирование экземпляра сервера вручную

После установки IBM Spectrum Protect версии 8.1.5 вы можете сконфигурировать IBM Spectrum Protect вручную, а не при помощи мастера по конфигурированию.

- Windows: Создание экземпляра сервера
  Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.
- Операционные системы WindowsWindows: Конфигурирование связи между сервером и клиентом
  После установки сервера вы можете настроить связь клиента с сервером, задав опции в файлах опций сервера и клиента.
- Windows: Форматирование базы данных и журнала
  Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.
- Windows: Подготовка менеджера базы данных к резервному копированию базы данных
  Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Windows: Создание экземпляра сервера

Создайте экземпляр IBM Spectrum Protect, введя команду db2icrt.

Об этой задаче

На одной рабочей станции может быть один или несколько экземпляров сервера.
Операционные системы WindowsВажное замечание: Прежде чем вводить команду db2icrt, убедитесь в следующем:

- Убедитесь, что существует каталог пользователя и каталог экземпляра для пользователя. Если каталога экземпляра нет, вы должны его создать.
  В каталоге экземпляра хранятся следующие файлы для экземпляра сервера:
  - Файл серверных опций, dsmserv.opt
  - Файл базы данных ключей сервера `cert.kdb` и файлы `.arm` (используемые клиентами и другими серверами для импорта сертификатов SSL на сервер)
  - Файл конфигурации устройств, если серверная опция DEVCONFIG не задает полное имя
  - Файл истории томов, если серверная опция VOLUMEHISTORY не задает полное имя
  - Тома для пулов хранения DEVTYPE=FILE, если спецификация каталога для класса устройств не является полной.

    - Обработчики пользователя
    - Выходная информация трассировки (если не задано полное имя)
- Сохраните резервную копию следующих файлов в безопасном и защищенном месте:
    - Файлы главного ключа шифрования (`dsmkeydb.*`)
    - Сертификат сервера и файлы секретных ключей (`cert.*`)

Операционные системы Windows

1. Войдите в систему как администратор и создайте экземпляр IBM Spectrum Protect при помощи команды db2icrt. Введите указанную ниже команду в виде одной строки. Учетная запись пользователя, которую вы укажете, станет ID пользователя-владельцем сервера Версии 8.1.5 (ID пользователя экземпляра).

   ```
   db2icrt -u учетная_запись_пользователя имя_экземпляра
   ```

   Например, если учетная запись пользователя - *tsminst1*, а экземпляр сервера - *Server1*, введите следующую команду:

   ```
   db2icrt -u tsminst1 server1
   ```

   Вас попросят ввести пароль для ID пользователя *tsminst1*. Потом, когда вы будете создавать и форматировать базу данных, вы укажете имя экземпляра, использовавшееся в этой команде, при помощи опции -k.
2. Измените путь по умолчанию для базы данных, так чтобы он указывал на диск, на котором находится каталог экземпляра сервера. Сделайте следующее:
    a. Выберите Пуск > Программы > IBM DB2 > DB2TSM1 > Инструменты командной строки > Процессор командной строки.
    b. Введите `quit`, чтобы закрыть процессор командной строки.

       Должно быть открыто окно командной строки с правильно сконфигурированной средой для успешного ввода команд в последующих шагах.

    c. В командной строке в этом окне введите указанную ниже команду, чтобы задать переменную среды для экземпляра сервера, с которым вы работаете:

       ```
       set db2instance=имя_экземпляра
       ```

       Значение *имя_экземпляра* совпадает с именем экземпляра, указанным вами при вводе команды db2icrt. Например, чтобы задать переменную среды для экземпляра сервера *Server1*, введите следующую команду:

       ```
       set db2instance=server1
       ```

    d. Введите команду, чтобы задать диск по умолчанию:

       ```
       db2 update dbm cfg using dftdbpath расположение_экземпляра
       ```

       Например, каталог экземпляра - d:\tsm\server1, а положение экземпляра - d:. Введите команду:

       ```
       db2 update dbm cfg using dftdbpath d:
       ```

3. Создайте новый файл серверных опций. Смотрите раздел Windows: Конфигурирование связи между сервером и клиентом.

Операционные системы Windows

Windows: Конфигурирование связи между сервером и клиентом

После установки сервера вы можете настроить связь клиента с сервером, задав опции в файлах опций сервера и клиента.

Об этой задаче

Задайте эти серверные опции до запуска сервера. При запуске сервера начнут действовать новые опции. Если вы измените какие-либо опции сервера после его запуска, вам придется остановить и перезапустить сервер, чтобы активировать обновленные опции.

Просмотрите файл опций сервера (`dsmserv.opt.smp`), расположенный в каталоге экземпляра сервера, чтобы взять оттуда значения опций связи сервера и указать их. По умолчанию сервер использует следующие способы связи: TCP/IP и именованные конвейеры.

Совет: Если при запуске консоли сервера вы видите сообщения с предупреждением, что протокол не может быть использован сервером, значит, протокол не установлен или настройки не соответствуют настройкам протоколаWindows.

Чтобы клиент мог использовать включенный на сервере протокол, файл опций клиента должен содержать соответствующие значения для опций связи. В файле опций сервера можно просмотреть эти значения для каждого протокола.

Можно задать один из следующих методов связи:

- TCP/IP версии 4 или версии 6
- Именованные каналы
- Совместное использование памяти
- Secure Sockets Layer (SSL)
  Совет: Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

-  Операционные системы WindowsWindows: Задание опций TCP/IP
  Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.
-  Операционные системы WindowsWindows: Как задать опции именованных конвейеров
  Метод связи с использованием именованных конвейеров идеально подходит в том случае, когда сервер и клиент запущены на одном компьютере под управлением Windows. Специальное конфигурирование для метода именованных конвейеров не требуется.
-  Операционные системы WindowsWindows: Задание опций Secure Sockets Layer
  Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Windows: Задание опций TCP/IP

Задайте опции TCP/IP для сервера IBM Spectrum Protect или сохраните опции, выбранные по умолчанию.

Об этой задаче

Ниже приводится пример списка опций TCP/IP, которые вы можете использовать для конфигурирования системы.

```
commmethod         tcpip
  tcpport            1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Совет: Можно использовать протокол TCP/IP версии 4, версии 6 или обеих версий.

TCPPORT
: Адрес порта сервера для взаимодействий TCP/IP и SSL. Значение по умолчанию - 1500.

 Операционные системы WindowsTCPWINDOWSIZE
:  Операционные системы WindowsЗадает размер буфера TCP/IP, используемого при отправке или приеме данных. Размер окна, используемого в сеансе, меньше размера окна для сервера и клиента. При большем размере окна используется дополнительная память, но это может способствовать повышению производительности.

  Чтобы использовать размер окна по умолчанию для операционной системы, задайте значение 0.

TCPNODELAY
: Позволяет указать, будет ли сервер отправлять сообщения малого объема, или же он разрешит TCP/IP буферизовать сообщения. При отправке небольших сообщений может повыситься пропускная способность, но при этом увеличится число пакетов, отправляемых по сети. Укажите YES, чтобы отправлять короткие сообщения, или NO, чтобы протокол TCP/IP сохранял их в буфере. Значение по умолчанию - YES.

TCPADMINPORT
: Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований связи с поддержкой TCP/IP или SSL, отличных от сеансов клиентов. Значением по умолчанию является значение TCPPORT.

SSLTCPPORT
: (Только SSL) Задает номер порта Secure Sockets Layer (SSL), на котором драйвер связи TCP/IP ожидает запросы на установление сеансов SSL от клиента резервного копирования и архивирования и клиента администрирования с интерфейсом командной строки.

SSLTCPADMINPORT
: (Только SSL) Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает запросов на установление сеансов SSL от клиента администрирования с интерфейсом командной строки.

Windows: Как задать опции именованных конвейеров

Метод связи с использованием именованных конвейеров идеально подходит в том случае, когда сервер и клиент запущены на одном компьютере под управлением Windows. Специальное конфигурирование для метода именованных конвейеров не требуется.

Об этой задаче

Вот пример задания метода именованных конвейеров:

```
commmethod namedpipe
     namedpipename              \\.\pipe\adsmpipe
```

COMMMETHOD можно использовать несколько раз в файле опций сервера IBM Spectrum Protect с различными значениями. Например, можно задать значения так:

```
commmethod        tcpip
commmethod namedpipe
```

Windows: Задание опций Secure Sockets Layer

Можно добавить дополнительную защиту данных и паролей с помощью протокола Secure Sockets Layer (SSL).

Прежде чем начать

SSL — это стандартная технология создания зашифрованных сеансов между серверами и клиентами. SSL предоставляет безопасный канал для связи серверов и клиентов по открытым путям связи. При использовании SSL идентификационная информация сервера проверяется с помощью цифровых сертификатов.

Чтобы обеспечить оптимальную производительность системы, используйте SSL только для сеансов, где это необходимо. Добавьте на сервер IBM Spectrum Protect дополнительные ресурсы процессора, чтобы удовлетворить возросшие требования.

Windows: Форматирование базы данных и журнала

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. При инициализации базы данных и журнала восстановления запрещаются все прочие операции сервера.

После конфигурирования связей сервера все готово для инициализации базы данных. Проверьте, что вы вошли в систему под ID пользователя экземпляра. Каталоги не должны находиться в файловых системах, где может закончиться свободное пространство. Если какие-либо каталоги (например, каталог архивного журнала) окажется недоступен или переполнен, сервер остановится.

 Операционные системы WindowsВажное замечание: Программа установки создает набор разделов реестра. Один из этих разделов указывает на каталог, в котором создан сервер по умолчанию с именем SERVER1. Чтобы установить дополнительный сервер, создайте каталог и запустите из этого каталога утилиту DSMSERV FORMAT с параметром -k. Этот каталог становится местом расположения сервера. Установленные серверы отслеживаются в реестре.

Как настроить обработчик списков завершения работы

Задайте для переменной реестра DB2NOEXITLIST значение ON для каждого экземпляра сервера. Войдите в систему от имени владельца экземпляра сервера и введите команду:

```
db2set -i имя_экземпляра_сервера
DB2NOEXITLIST=ON
```

Например:  Операционные системы Windows

```
db2set -i server1 DB2NOEXITLIST=ON
```

Инициализация экземпляра сервера

Чтобы инициализировать экземпляр сервера, используйте утилиту DSMSERV FORMAT. Например, если каталог экземпляра сервера - это */tsminst1*, введите следующие команды:Операционные системы Windows

```
cd \tsminst1
dsmserv -k server2 format dbdir=d:\tsm\db001 activelogsize=32768
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

Совет: Если вы зададите несколько каталогов, убедитесь, что размеры соответствующих файловых систем равны, что позволит обеспечить непротиворечивую степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.

Информация, связанная с данной:

DSMSERV FORMAT (форматирование базы данных и журнала)

Windows: Подготовка менеджера базы данных к резервному копированию базы данных

Чтобы создать резервную копию данных в базе данных для IBM Spectrum Protect, нужно разрешить менеджер базы данных и сконфигурировать интерфейс прикладного программирования (Application Programming Interface - API) IBM Spectrum Protect.

Об этой задаче

Если вы создаете экземпляр сервера IBM Spectrum Protect при помощи мастера по конфигурированию, то вам не нужно выполнять эти действия. Если вы конфигурируете экземпляр вручную, выполните описанные ниже шаги, прежде чем вводить команду BACKUP DB или RESTORE DB.

Внимание: Если база данных недоступна, весь сервер IBM Spectrum Protect становится недоступным. Если база данных утеряна и ее нельзя восстановить, может оказаться затруднительным или даже невозможным восстановить данные, которыми управляет этот сервер. Поэтому очень важно создать резервную копию базы данных.
Операционные системы WindowsОграничение: Резервное копирование и восстановление через совместно используемую память недоступно в системах Windows.
Операционные системы WindowsВ приведенных ниже примерах команд в качестве имени экземпляра базы данных используется значение `server1`, а в качестве каталога сервера IBM Spectrum Protect - d:\tsmserver1. Подставьте вместо этих значений в команды свои фактические значения.

1. Создайте в каталоге d:\tsmserver1 файл `tsmdbmgr.env` со следующим содержимым:

   ```
   DSMI_CONFIG=каталог_экземпляра_сервера\tsmdbmgr.opt
   DSMI_LOG=каталог_экземпляра_сервера
   ```

2. Задайте конфигурацию переменных среды API DSMI_ для экземпляра базы данных:
   a. Откройте окно команд DB2. Один из способов - перейти в каталог C:\Program Files\Tivoli\TSM\db2\bin или, если вы установили IBM Spectrum Protect в другой каталог - в подкаталог db2\bin в основном каталоге установки. Затем введите команду:

      ```
      db2cmd
      ```

   b. Введите команду:

      ```
      db2set -i server1 DB2_VENDOR_INI=d:\tsmserver1\tsmdbmgr.env
      ```

3. Создайте в каталоге d:\tsmserver1 файл `tsmdbmgr.opt` со следующим содержимым:

   ```
   ************************************************
   nodename $$_TSMDBMGR_$$
   commmethod         tcpip
   tcpserveraddr localhost
   tcpport            1500
   passwordaccess  generate
   errorlogname d:\tsmserver1\tsmdbmgr.log
   ```

   где
   - *nodename* задает имя узла, используемое API клиента для соединения с сервером во время резервного копирования базы данных. Для правильной работы резервного копирования базы данных это значение

должно быть `$$_TSMDBMGR_$$`.
- *commethod* задает API клиента, используемый для соединения с сервером для резервного копирования базы данных.
- *tcpserveraddr* задает адрес сервера, который API клиента будет использовать для связи с сервером для резервного копирования базы данных. Для резервного копирования базы данных надо задать значение `localhost`.
- *tcpport* задает номер порта, который API клиента будет использовать для связи с сервером с целью резервного копирования базы данных. Значение `tcpport` должно быть значением, которое задано в файле опций сервера dsmserv.opt.
- Опция *passwordaccess* требуется для подключения резервного узла к серверу в системах под управлением Windows.
- *errorlogname* задает журнал ошибок, в который API клиента будет записывать ошибки, происходящие при резервном копировании базы данных. Обычно этот журнал находится в каталоге экземпляра сервера. Однако его можно поместить в любой другой каталог, разрешения на запись в который есть у ID пользователя.

Windows: Опции конфигурирования сервера для обслуживания сервера баз данных

Чтобы избежать проблем с ростом базы данных и производительности сервера, сервер автоматически отслеживает таблицы своих баз данных и реорганизует их по мере надобности. Перед переводом сервера в производственный режим задайте опции сервера, управляющие временем реорганизации. Если вы собираетесь использовать дедупликацию данных, убедитесь, что включена опция запуска реорганизации индексов.

Об этой задаче

Для реорганизации таблиц и индексов требуются значительные процессорные ресурсы, пространство для активного журнала и пространство для архивного журнала. Поскольку резервное копирование баз данных имеет приоритет перед реорганизацией, выберите время и длительность для реорганизации так, чтобы эти процессы не перекрывались и реорганизация смогла завершиться.

 Операционные системы WindowsВы можете оптимизировать реорганизацию индекса и таблиц для базы данных сервера. Таким образом можно избежать неожиданного роста базы данных и проблем, отрицательно влияющих на производительность. Инструкции смотрите в техническом примечании 1683633.

Если вы изменяете эти опции сервера при работающем сервере, надо остановить и перезапустить сервер, чтобы они вступили в силу.

Процедура

1. Измените опции сервера.
   Операционные системы WindowsОтредактируйте файл опций сервера dsmserv.opt в каталоге экземпляра сервера при помощи текстового редактора. При изменении файла опций сервера придерживайтесь следующих рекомендаций:
   - Чтобы включить опцию, удалите звездочку в начале строки.
   - Введите опцию в любой строке.
   - Вводите по одной опции на строке. Вся опция со своим значением должна быть записана на одной строке.
   - Если для одной опции в файле есть несколько записей, сервер использует последнюю запись.

   Чтобы просмотреть доступные опции сервера, воспользуйтесь файлом примера dsmserv.opt.smp в каталоге c:\Program Files\Tivoli\TSM.
2. Если вы собираетесь использовать дедупликацию данных, то разрешите опцию сервера ALLOWREORGINDEX. Добавьте следующую опцию и значение в файл опций сервера:

   ```
   allowreorgindex yes
   ```

3. Задайте опции сервера REORGBEGINTIME и REORGDURATION, управляющие моментом начала реорганизации и ее длительностью. Выберите время и длительность, чтобы выполнять реорганизацию во время ожидаемой минимальной занятости сервера. Эти опции сервера действуют на процессы реорганизации как таблиц, так и индексов.
   a. Задайте время начала реорганизации при помощи опции сервера REORGBEGINTIME. Задайте время по 24-часовой системе. Например, чтобы начать реорганизацию в 8.30 вечера, задайте в файле опций сервера:

```
reorgbegintime 20:30
```

b. Задайте интервал, в который сервер может начать реорганизацию. Например, чтобы указать, что сервер может начать реорганизацию в течении четырех часов после времени, заданного опцией сервера REORGBEGINTIME, задайте в файле опций сервера:

```
reorgduration 4
```

4. Если в момент изменения файла опций сервера сервер работает, остановите и перезапустите его.

 Операционные системы Windows

Windows: Запуск экземпляра сервера в системах Windows

В производственной среде предпочтительным методом запуска сервера является запуск его как службы Windows. В среде, где вы производите переконфигурирование или тестирование либо выполняете задачи по обслуживанию, запускайте сервер в приоритетном режиме или используйте режим обслуживания.

Прежде чем начать

Выберите один из следующих способов запуска сервера:

Как службы Windows
: Этот метод удобен для использования в производственной среде. Если вы конфигурируете сервер для запуска как службы, то можно указать, что сервер должен автоматически запускаться при запуске системы.

В режиме активного окна
: Этот метод удобен при конфигурировании или при тестировании сервера. При запуске сервера в режиме активного окна IBM Spectrum Protect предоставляет специальный ID пользователя-администратора: SERVER_CONSOLE. Все сообщения сервера показываются в активном окне. Эти сообщения могут быть полезны для отладки проблем запуска.

В режиме обслуживания
: Этот метод полезен при выполнении задач по обслуживанию или переконфигурированию. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Процедура

Выполните инструкции для выбранной опции:

Опция	Описание
Запуск сервера как службы Windows	Для запуска сервера как службы Windows выполните одно из следующих действий: • Если вы сконфигурировали сервер при помощи мастера конфигурирования, выполните следующие действия: a. Сконфигурируйте сервер для запуска как службы Windows, выполнив инструкции в разделе Windows: Конфигурирование сервера для запуска как службы Windows. b. Запустите сервер, выполнив инструкции в разделе Windows: Запуск сервера как службы Windows. • Если вы не использовали мастер конфигурирования, создайте и сконфигурируйте службу Windows, выполнив инструкции в разделе Windows: Создание и конфигурирование службы Windows вручную.
Запуск сервера в режиме активного окна	Чтобы запустить сервер в режиме активного окна, выполните инструкции в разделе Windows: Запуск сервера в режиме активного окна.
Запуск сервера в режиме обслуживания	Чтобы запустить сервер в режиме обслуживания, следуйте инструкциям в разделе Windows: Запуск сервера в режиме обслуживания.

 Операционные системы Windows

Windows: Конфигурирование сервера для запуска как службы Windows

Чтобы запустить сервер как службу Windows, нужно правильно задать опции и права доступа.

Прежде чем начать

Нужно создать службу Windows. Если вы сконфигурировали сервер при помощи мастера конфигурирования, служба Windows была создана автоматически. В этом случае используйте эту процедуру, чтобы сконфигурировать сервер для запуска как службы Windows.

Если вы не использовали мастер, то нужно вручную создать и сконфигурировать службу Windows, выполнив действия из раздела Windows: Создание и конфигурирование службы Windows вручную.

Процедура

1. В меню Windows Пуск выберите Выполнить, введите `services.msc` и нажмите кнопку OK.
2. В окне Службы выберите экземпляр сервера, который вы хотите запускать как службу, и откройте окно Свойства. Например, выберите TSM INST1 и откройте Свойства.
3. Чтобы убедиться, что служба сервера запускается автоматически, щелкните по вкладке Общие. В списке Тип запуска выберите Автоматически.
4. Чтобы задать пользователя для запуска службы сервера, щелкните по вкладке Вход в систему и выполните одно из следующих действий:
   - Чтобы запустить службу сервера с учетной записью Local System, выберите Учетная запись Local System и щелкните по OK.
   - Чтобы запустить службу сервера с ID пользователя экземпляра, сделайте следующее:
     a. Включите радиокнопку С учетной записью и (нажав кнопку Обзор...) найдите ID пользователя - владельца экземпляра DB2 сервера с разрешениями запускать сервер.
     b. В окне Выбор: Пользователь в поле Введите имена выбираемых объектов введите ID пользователя.
     c. Нажмите кнопку Проверить имена.
     d. Дважды щелкните по OK.
5. Если вы сконфигурировали сервер для запуска с учетной записью Local System , то предоставьте базе данных доступ к учетной записи Local System:
   a. Войдите в систему от имени ID пользователя, использовавшегося для создания базы данных сервера. Это ID пользователя, использовавшийся для запуска утилиты DSMSERV FORMAT для инициализации базы данных сервера. Если сервер был сконфигурирован при помощи мастера конфигурирования dsmicfgx, то это ID пользователя, использовавшийся для создания экземпляра.
   b. Откройте окно команд DB2. Если сервер установлен в Windows Server 2012, откройте окно Пуск и выберите Командное окно DB2 - Администратор.
   c. В командном окне DB2 введите следующие команды:

```
set DB2INSTANCE=server1
db2 connect to TSMDB1
db2 grant dbadm with dataaccess with accessctrl on database to user system
db2 grant secadm on database to user system
```

   Совет: После конфигурирования службы сервера для запуска под локальной системной учетной записью доступ к базе данных будет у всех администраторов в системе. Кроме того, сервер может запустить любой администратор, который может войти в систему.

Дальнейшие действия

Чтобы запустить службу, выполните инструкции из раздела Windows: Запуск сервера как службы Windows.
 Операционные системы Windows

Windows: Запуск сервера как службы Windows

Если IBM Spectrum Protect запускается в системе Windows, сервер можно запустить как службу.

Прежде чем начать

Нужно создать службу Windows. Служба создается автоматически при конфигурировании сервера с использованием мастера конфигурирования. Если служба была создана автоматически, то нужно сконфигурировать сервер, чтобы он запускался как служба, выполнив действия из раздела Windows: Конфигурирование сервера для запуска как службы Windows. После этого используйте эту процедуру для запуска сервера как службы.

Если вы не использовали мастер конфигурирования для создания службы, службу нужно создать и сконфигурировать вручную. Выполните действия, описанные в разделе Windows: Создание и конфигурирование службы Windows вручную.

Процедура

Чтобы запустить сервер как службу Windows, выполните следующие действия:

1. Войдите в систему сервера, используя ID пользователя из группы администраторов.
2. В меню Windows Пуск выберите Выполнить, введите `services.msc` и нажмите кнопку OK.
3. В окне Службы выберите экземпляр сервера, который вы хотите запустить, и нажмите кнопку Запустить.

Дальнейшие действия

Поскольку служба сервера может генерировать запросы, требующие ответных действий, работу сервера важно отслеживать при помощи Центра операций или клиента администрирования.

Для просмотра сообщений об успешном запуске и останове, записываемых в журнал прикладных программ Windows, используйте средство просмотра событий в папке Администрирование.

 Операционные системы Windows

Windows: Создание и конфигурирование службы Windows вручную

Если вы сконфигурировали сервер при помощи мастера конфигурирования, то служба Windows была создана автоматически. Если служба не создана автоматически, то ее нужно создать.

Прежде чем начать

Для этого войдите в систему в ID пользователя из группы Администраторы.

Процедура

Чтобы создать службу Windows и сконфигурировать для службы опции запуска, сделайте следующее:

Откройте командное окно и введите команду sc.exe create:

```
sc.exe create имя_сервера binPath= "каталог_сервера -k
имя_экземпляра"
start= тип_запуска obj= имя_учетной_записи password= пароль
```

Здесь используются следующие обозначения:

имя_сервера
: Имя службы сервера.

каталог_сервера
: Полное имя выполняемого файла dsmsvc.exe. Каталог по умолчанию:

  C:\Program Files\Tivoli\TSM\server

имя_экземпляра
: Имя экземпляра DB2 (например, Server1); это также имя экземпляра сервера.

тип_запуска
: Метод запуска службы. Для автоматического запуска службы введите `auto`. Если задано `auto`, то служба автоматически запускается при запуске системы и автоматически перезапускается при перезапуске системы. Для запуска службы вручную введите `demand`.

имя_учетной_записи
: ID пользователя для учетной записи, с которой запускается служба. Например, именем учетной записи может быть Administrator. Это необязательный параметр. Если параметр не задан, то используется учетная запись Local System.

пароль

Пароль для учетной записи *имя_учетной_записи*.

Совет: При вводе команды вставляйте пробел после каждого символа равенства (=).

Результаты

Сервер запускается как служба Windows.
 Операционные системы Windows

Windows: Запуск сервера в режиме активного окна

Для непосредственного взаимодействия с сервером IBM Spectrum Protect запускайте его в режиме активного окна. Например, запустите сервер в режиме активного окна, если вы хотите вводить команды.

Процедура

1. Перейдите в каталог, в котором установлен сервер. Например, перейдите в каталог c:\program files\tivoli\tsm\server.
2. Введите команду

   ```
   dsmserv -k имя_экземпляра
   ```

   где *имя_экземпляра* задает экземпляр сервера.

 Операционные системы Windows

Windows: Службы, связанные с сервером в системах Windows

При запуске сервера IBM Spectrum Protect в качестве службы другие службы запускаются автоматически. Эти службы связаны с менеджером базы данных, DB2.

С сервером связаны следующие службы:

Имя службы	Назначение	Замечания
TSM *экземпляр_сервера*	Служба для экземпляра сервера с именем *экземпляр_сервера*. Например: TSM Server1	Задайте для этой службы опции запуска и остановки, так чтобы экземпляр сервера запускался автоматически. Каждый экземпляр сервера работает как отдельная служба.
DB2 - DB2TSM1 - *ЭКЗЕМПЛЯР_СЕРВЕРА*	Служба DB2 для экземпляра сервера с именем *экземпляр_сервера*. Например: DB2 - DB2TSM1 - SERVER1	Эта служба автоматически запускается при запуске экземпляра сервера. Служба DB2 не останавливается автоматически при остановке службы сервера. В системе существует одна из этих служб для каждой службы экземпляра сервера, запущенного в системе.
DB2 Governor (DB2TSM1)	Служба DB2, создаваемая во время установки и необходимая для всех экземпляров сервера.	Не изменяйте опции для этой службы.
DB2 License Server (DB2TSM1)	Служба DB2, создаваемая во время установки и необходимая для всех экземпляров сервера.	Не изменяйте опции для этой службы.
DB2 Management Server (DB2TSM1)	Служба DB2, создаваемая во время установки и необходимая для всех экземпляров сервера.	Не изменяйте опции для этой службы.
DB2 Remote Command Server (DB2TSM1)	Служба DB2, создаваемая во время установки и необходимая для всех экземпляров сервера.	Не изменяйте опции для этой службы.

 Операционные системы Windows

Windows: Запуск сервера в режиме обслуживания

Сервер можно запустить в режиме обслуживания, чтобы избежать повреждений при выполнении задач по обслуживанию и переконфигурированию.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

   ```
   halt
   ```

2. Запустите сервер, используя метод, который вы используете в производственном режиме.

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Windows: Остановка сервера

При необходимости сервер можно остановить, чтобы передать управление операционной системе. Чтобы предотвратить отключение административных и клиентских узлов, останавливайте сервер только после завершения или отмены текущих сеансов.

Об этой задаче

Чтобы остановить сервер, введите в командной строке IBM Spectrum Protect следующую команду:

```
halt
```

Windows: Регистрация лицензий

Сразу же зарегистрируйте все лицензированные функции IBM Spectrum Protect, которые вы приобрели, чтобы не потерять никаких данных после начала выполнения сервером таких операций, как резервное копирование ваших данных.

Об этой задаче

Используйте для этого команду REGISTER LICENSE. Дополнительные сведения смотрите в разделе REGISTER LICENSE.

Пример: Зарегистрировать лицензию

Зарегистрируйте базовую лицензию на IBM Spectrum Protect.

```
register license file=tsmbasic.lic
```

Windows: Подготовка сервера к операциям резервного копирования базы данных

Чтобы подготовить сервер к автоматическим и ручным операциям резервного копирования базы данных, убедитесь, что вы указали класс ленточных или файловых устройств, а также выполните другие шаги.

Процедура

1. Убедитесь, что конфигурация IBM Spectrum Protect - полная. Если вы не используете мастер конфигурирования (dsmicfgx) для конфигурирования сервера, убедитесь, что вы выполнили шаги по конфигурированию сервера вручную для резервного копирования базы данных.
2. Выберите класс устройств, который следует использовать для резервного копирования базы данных, защитите главный ключ шифрования и задайте пароль. Все эти действия выполняются путем ввода команды SET DBRECOVERY из административной командной строки:

   ```
   set dbrecovery имя_класса_устройств protectkeys=yes password=имя_пароля
   ```

   где *имя_класса_устройств* задает класс устройств, который следует использовать для операций резервного копирования базы данных, а *имя_пароля* задает пароль.
   Вы обязательно должны задать имя класса устройств, иначе резервное копирование завершится неудачно. Задав PROTECTKEYS=YES, вы сделаете так, что во время операций резервного копирования базы данных будет создаваться резервная копия главного ключа шифрования.
   Важное замечание: Создайте надежный пароль, содержащий хотя бы 8 символов. Убедитесь, что вы запомнили этот пароль. Если задан пароль для резервной копии базы данных, вы должны указать тот же самый пароль в команде RESTORE DB для восстановления базы данных.

Пример

Чтобы указать, что резервные копии базы данных содержат копию главного ключа шифрования для сервера, введите следующую команду:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Windows: Запуск нескольких экземпляров серверов на одном компьютере

Вы можете создать несколько экземпляров сервера в системе. У каждого экземпляра сервера будет свой отдельный каталог экземпляра и свои отдельные каталоги базы данных и журнала.

Умножьте требования к памяти и другим системным ресурсам для одного сервера на число экземпляров, которые вы собираетесь создать в системе.

 Операционные системы WindowsНабор файлов для одного экземпляра сервера хранится отдельно от файлов, используемым другим экземпляром сервера в той же системе. Выполните для каждого нового экземпляра шаги, описанные в разделе Windows: Создание экземпляра сервера, включая (по желанию) создание пользователя нового экземпляра.

Чтобы управлять объемом системной памяти, используемым каждым сервером, задайте опцию DBMEMPERCENT, позволяющую ограничить процент системной памяти. Если все серверы равноценны, используйте для всех серверов

одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.

Можно произвести обновление V7.1 до V8.1 напрямую. Более подробную информацию смотрите в разделе об обновлении (Обновление до V8.1). Если при обновлении в вашей системе есть несколько серверов, запускать мастер установки нужно только один раз. Мастер установки соберет информацию о базах данных и переменных для всех исходных экземпляров сервера.

Если вы выполняете обновление IBM Spectrum Protect V6.3 до V8.1.5 и в системе есть несколько серверов, то все экземпляры, существующие в DB2 V9.7, удаляются и заново создаются в DB2 V11.1. Мастер сгенерирует команду `db2 upgrade db имя_бд` для каждой базы данных. В процессе обновления также будет произведено переконфигурирование переменных среды базы данных для каждого экземпляра в вашей системе.

 Операционные системы WindowsВ типичном сценарии установки IBM Spectrum Protect описывается один экземпляр сервера, устанавливаемый на компьютер сервера IBM Spectrum Protect. При конфигурировании в кластерной среде вам может потребоваться установить второй экземпляр. При наличии нескольких библиотек магнитных лент или конфигурации с использованием только жестких дисков может также потребоваться запускать несколько серверов на одном мощном компьютере. После установки и конфигурирования первого сервера IBM Spectrum Protect используйте мастер инициализации серверов для создания дополнительных экземпляров сервера IBM Spectrum Protect на том же компьютере.

 Операционные системы WindowsИспользуя мастер инициализации серверов, можно установить до четырех экземпляров сервера IBM Spectrum Protect в одной системе или в кластере.

Задачи, связанные с данной:
Запуск нескольких экземпляров серверов на одном компьютере (V7.1.1)

Windows: Мониторинг сервера

Когда вы начнете использовать сервер в производственном режиме, отслеживайте пространство, используемое сервером, чтобы убедиться, что объем пространства достаточен. Если нужно, то настройте пространство.

Процедура

1. Следите за активным журналом, чтобы убедиться, что его размер соответствует рабочей нагрузке, обрабатываемой экземпляром сервера.

   Если уровень рабочей нагрузки на сервер приближается к типичному ожидаемому уровню, то объем пространства, используемого активным журналом, составляет 80-90% пространства. В этот момент, возможно, нужно увеличить объем пространства. Необходимость увеличения пространства зависит от типов транзакций, составляющих рабочую нагрузку сервера. Характеристики транзакций влияют на то, как используется пространство активного журнала.

   На использованием пространства активного журнала могут влиять следующие характеристики транзакций:

   - Число и размер файлов в операциях резервного копирования.
     - Такие клиенты, как файл-серверы, которые создают резервные копии большого числа мелких файлов, могут инициировать большое число быстро завершающихся транзакций. Транзакции могут использовать большой объем пространства в активном журнале, но кратковременно.
     - Такие клиенты, как почтовый сервер или сервер базы данных, которые создают резервные копии больших объемов данных в ходе немногочисленных транзакций, могут инициировать небольшое число транзакций, для завершения которых требуется длительное время. Транзакции могут использовать небольшой объем пространства в активном журнале, но в течение длительного времени.
   - Типы соединений с сетью
     - Транзакции, связанные с операциями резервного копирования, которые выполняются с использованием высокоскоростных сетевых соединений, завершаются быстрее. Транзакции используют пространство в активном журнале в течение более короткого времени.
     - Для завершения транзакций, связанных с операциями резервного копирования, которые выполняются с использованием относительно низкоскоростных сетевых соединений, требуется больше времени. Транзакции используют пространство в активном журнале в течение более длительного времени.

   Если сервер обрабатывает транзакции с широким диапазоном характеристик, то пространство, используемое для активного журнала, может значительно увеличиваться и уменьшаться с течением времени. В этом случае вы

должны сделать так, чтобы, как правило, использовался меньший процент пространства активного журнала. Дополнительное пространство позволит активному журналу увеличиваться в размере, если для выполнения транзакций требуется очень много времени.

2. Следите за архивным журналом, чтобы убедиться в том, что для него всегда хватает места.
   Напоминание: Если архивный журнал и архивный журнал отказоустойчивости заполнятся, может заполниться активный журнал, и сервер остановится. Цель заключается в том, чтобы архивному журналу был доступен достаточный объем пространства и он никогда не использовал все доступное ему пространство.
   Вы, вероятно, заметите следующие закономерности:
   a. Сначала архивный журнал быстро растет по мере выполнения операций резервного копирования клиента.
   b. Резервное копирование базы данных производится регулярно либо по расписанию, либо вручную.
   c. После выполнения, как минимум, двух операций полного резервного копирования базы данных сокращение журналов происходит автоматически. В результате отбрасывания пространство, используемое архивным журналом, уменьшается.
   d. Обычные операции клиента продолжаются, и архивный журнал снова растет.
   e. Резервное копирование базы данных выполняется регулярно, и отбрасывание журналов происходит так же часто, как и операции полного резервного копирования базы данных.

   При таких закономерностях архивный журнал сначала растет, затем уменьшается, а затем может снова вырасти. С течением времени, по мере продолжения нормальной работы, объем пространства, используемого архивным журналом, должен достичь относительно постоянного уровня.

   Если архивный журнал продолжает расти, то выполните одно из описанных ниже действий или оба эти действия:
   - Добавьте пространство для архивного журнала. Это может означать перемещение архивного журнала в другую файловую систему.
   - Увеличьте частоту полного резервного копирования базы данных, чтобы отбрасывание журналов производилось чаще.
3. Если вы задали каталог для резервного архивного журнала, определите, сохраняются ли в этом каталоге какие-либо журналы при обычной работе. Если пространство резервного журнала используется, то увеличьте размер архивного журнала. Цель состоит в том, чтобы резервный архивный журнал использовался только в экстраординарных условиях, а не при обычной работе.

Windows: Установка пакета исправлений сервера IBM Spectrum Protect

Служебные обновления программного обеспечения IBM Spectrum Protect, также называемые пакетами Fix Pack, выводят сервер на текущий служебный уровень.

Прежде чем начать

Чтобы установить на сервер пакет Fix Pack или промежуточный пакет исправлений, установите сервер требуемого для выполнения уровня. Не обязательно запускать установку сервера на уровне базового выпуска. Например, если у вас установлена версия 8.1.1, то можно перейти сразу к самому последнему пакету Fix Pack для V8.1. Не обязательно начинать с установки V8.1.0, если доступно текущее изменение.

У вас должен быть установлен пакет лицензий IBM Spectrum Protect. Пакет лицензий приобретается вместе с базовым выпуском программного обеспечения. При загрузке пакета исправлений или промежуточного пакета исправлений с сайта Fix Central установите лицензию на сервер, которая есть на веб-сайте Passport Advantage. Для вывода сообщений и справки на языке, ином чем американский английский, установите языковый пакет по своему выбору.

Если вы обновляете сервер до V8.1.5 или новее, а затем возвращаетесь к уровню сервера, более раннему, чем V8.1.5, необходимо восстановить базу данных на момент времени, предшествующий обновлению. Во время процесса обновления выполните требуемые действия, обеспечивающие возможность восстановления базы данных: создайте резервные копии базы данных, файла хронологии тома, файла конфигурации устройств и файла опций сервера. Дополнительные сведения смотрите в разделе Windows: Возврат от версии 8.1.5 к предыдущему серверу.

Если вы используете службу управления клиентами, убедитесь, что вы обновили ее до той же версии, к которой относится сервер IBM Spectrum Protect.

Убедитесь, что вы сохранили установочный носитель базового выпуска установленного сервера. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится

неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.

Посетите страницу Портал поддержки IBM® и найдите там следующую информацию:

- Список последних исправлений и их скачивание. Щелкните по **Downloads** (Материалы для скачивания) и примените все соответствующие исправления.
- Подробности получения базового пакета лицензий. Найдите **Downloads > Passport Advantage** (Материалы для скачивания - Passport Advantage).
- Поддерживаемые платформы и системные требования. Укажите для поиска: **поддерживаемые операционные системы IBM Spectrum Protect**.

Обязательно обновите сервер, прежде чем обновлять клиенты резервного копирования и архивирования. Если не обновить сначала сервер, связь между серевром и клиентами может прерваться.

Внимание: Не изменяйте программу DB2, устанавливаемую вместе с пакетами установки и пакетами исправлений IBM Spectrum Protect. Не устанавливайте другую версию, выпуск или пакет исправлений и не производите обновление до другой версии, выпуска или пакета исправлений программы DB2, так как это может привести к повреждению базы данных.

Процедура

Чтобы установить пакет исправлений или промежуточное исправление, сделайте следующее:

1. Создайте резервную копию базы данных. Рекомендуется способ использовать резервное копирование в режиме снимка. Резервное копирование в режима снимка - это полное резервное копирование базы данных, не прерывающее никаких плановых операций резервного копирования базы данных. Например, введите следующую команду управления IBM Spectrum Protect:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте резервную копию информации о конфигурации устройств. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup devconfig filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
3. Сохраните файл хронологии томов в другом положении или переименуйте этот файл. Введите следующую команду управления IBM Spectrum Protect:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt. Этот файл расположен в каталоге экземпляра сервера.
5. Прежде чем устанавливать пакет исправлений или промежуточное исправление, остановите сервер. Используйте команду HALT.
6. Убедитесь, что в каталоге установки доступно дополнительное пространство. Установка этого пакета Fix Pack может потребовать дополнительного временного дискового пространства в каталоге установки сервера. Объем дополнительного дискового пространства может быть таким же, как требуется для установки новой базы данных как части установки IBM Spectrum Protect. Мастер по установке IBM Spectrum Protect показывает объем пространства, требуемого для установки пакета Fix Pack, и доступный объем пространства. Если требуемый объем пространства превышает доступный, установка прекращается. Если установка остановилась, добавьте требуемое дисковое пространство к файловой системе и перезапустите установку.
7. Получите файл пакета исправлений или промежуточного исправления, который вы хотите установить, со страниц Портал поддержки IBM, Passport Advantage или Fix Central.
8.  Операционные системы WindowsПерейдите в каталог, куда вы поместили исполняемый файл. Затем, чтобы извлечь файлы программы установки, либо дважды щелкните по указанному ниже исполняемому файлу, либо введите приведенную ниже команду в командной строке.
   Совет: Файлы извлекаются в текущий каталог. Убедитесь, что исполняемый файл находится в каталоге, куда будут извлекаться файлы.

   ```
   8.x.x.x-IBM-SPSRV-платформа.exe
   ```

   где: *платформа* - это операционная система, в которой устанавливается IBM Spectrum Protect.
9. Выберите один из следующих способов установки IBM Spectrum Protect.

Важное замечание: После установки пакета исправлений не нужно снова выполнять все шаги по конфигурированию. Вы можете остановить программу после завершения установки, исправить все ошибки и перезапустить свои серверы.
Установите программное обеспечение IBM Spectrum Protect одним из следующих способов:

Мастер установки
: Выполните инструкции для вашей операционной системы.
Windows: Установка IBM Spectrum Protect при помощи мастера установки

Совет: Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.

Командная строка в режиме консоли
: Выполните инструкции для вашей операционной системы.
Windows: Установка IBM Spectrum Protect в режиме консоли

Режим без вывода сообщений
: Выполните инструкции для вашей операционной системы.
Windows: Установка IBM Spectrum Protect в режиме без вывода сообщений

Совет: Если в вашей системе используется несколько экземпляров сервера, запустите мастер установки только один раз. Мастер по установке обновит все экземпляры сервера.

Результаты

Исправьте ошибки, обнаруженные в процессе установки.

Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по Файл > Просмотреть журнал. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по Справка > Экспорт данных для анализа ошибок.

Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:

- Операционные системы WindowsC:\ProgramData\IBM\Installation Manager\logs
- Операционные системы WindowsWindows: Применение пакета Fix Pack к IBM Spectrum Protect 8.1.5 в кластерной среде для Windows
  Для использования новых функций продукта можно обновить сервер, установленный в операционной системе Windows в кластерной среде, с версии 6 или 7.1 до IBM Spectrum Protect версии 8.1.5.

Windows: Возврат от версии 8.1.5 к предыдущему серверу

Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.

Прежде чем начать

У вас должны быть следующие элементы для более ранней версии сервера:

- Резервная копия базы данных сервера
- Файл хронологии тома
- Файл конфигурации устройств
- Файл серверных опций

Об этой задаче

Используйте одни и те же инструкции и для возврата к прежней версии в пределах одного выпуска (например, от 8.1.3 до 8.1.2 или от 8.1.3 до 7.1.2). Прежняя версия должна совпадать с версией, использовавшейся перед обновлением до версии 8.1.

Внимание: Задайте значение параметра REUSEDELAY, помогающее предотвратить потерю данных клиента резервного копирования и архивирования при возврате сервера к прежней версии.

- Операционные системы WindowsWindows: Возврат к предыдущей версии сервера в кластерной конфигурации
  Если после обновления требуется вернуться к прежней версии сервера, у вас должна быть полная резервная копия базы данных из исходной версии. Необходим также носитель для установки исходной версии сервера и ключевые файлы конфигурации. Тщательно выполняйте подготовительные действия перед обновлением сервера. В этом случае можно будет вернуться к прежней версии сервера IBM Spectrum Protect с минимальной потерей данных.

Шаги по возврату к предыдущей версии сервера

Об этой задаче

Выполните следующие действия в системе, где установлен сервер версии 8.1:

Процедура

1. Остановите сервер, чтобы закрыть все операции сервера, с помощью команды HALT.
2. Удалите базу данных из менеджера базы данных, затем удалите каталоги базы данных и журналов восстановления.
   a. Вручную удалите базу данных. Один из способов удалить ее - ввести следующую команду:
   Операционные системы Windows

   ```
   dsmserv -k имя_экземпляра removedb tsmdb1
   ```

   b. Если вам нужно снова использовать пространство, занятое каталогами базы данных и журналов восстановления, вы теперь можете удалить эти каталоги.
3. Деинсталлируйте сервер V8.1 при помощи программы деинсталляции. При деинсталляции удаляется сервер и менеджер баз данных вместе с их каталогами. Дополнительные сведения смотрите в разделе Windows: Деинсталляция IBM Spectrum Protect.
4. Остановите службу кластеров. Заново установите версию программы сервера, которую вы использовали перед обновлением до V8.1.5. Эта версия должна совпадать с версией вашего сервера на момент создания резервной копии базы данных, которую вы восстановите в одном из последующих шагов. Например, перед обновлением сервер относился к версии 7.1.7, а вы собираетесь применить резервную копию базы данных, использовавшуюся на этом сервере. Чтобы получить возможность восстанавливать эту резервную копию базы данных, нужно установить Fix Pack для V7.1.7.
5. Сконфигурируйте новую базу данных сервера при помощи мастера конфигурирования. Чтобы запустить мастер, введите следующую команду: Операционные системы Windows

   ```
   /dsmicfgx
   ```

6. Убедитесь, что нет серверов, запущенных в фоновом режиме.
7. Восстановите базу данных на заданный момент времени перед обновлением.
8. Скопируйте следующие файлы в каталог экземпляра.
   - Файл конфигурации устройств
   - Файл хронологии тома
   - Файл опций сервера (обычно, dsmserv.opt)
9. Если вы включили дедупликацию данных для каких-либо пулов хранения типа FILE, которые существовали перед обновлением, или если вы при использовании сервера V8.1.5 перенесли данные, существовавшие перед обновлением, в новые пулы хранения, вы должны будете выполнить дополнительные шаги по восстановлению. Дополнительные сведения смотрите в разделе Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных.
10. Если значение параметра REUSEDELAY для пулов хранения меньше возраста восстанавливаемой вами базы данных, восстановите тома во всех пулах хранения с последовательным доступом, которые были консолидированы после резервного копирования базы данных. Используйте команду RESTORE VOLUME.
    Если у вас нет резервной копии пула хранения, произведите аудит консолидированных томов при помощи команды AUDIT VOLUME с параметром FIX=YES для устранения противоречий. Например:

    ```
    audit volume имя_тома fix=yes
    ```

11. Если с использованием сервера версии 8.1 выполнялись операции резервного копирования или архивирования клиента, выполните аудит томов пулов хранения, на которых были сохранены эти данные.

Дополнительные шаги по восстановлению, если вы создавали новые пулы хранения или включали дедупликацию данных

Если во время работы сервера в версии 8.1.5 вы создавали новые пулы хранения, включали дедупликацию данных для любых пулов хранения типа FILE или совершали оба этих действия, необходимо выполнить некоторые дополнительные шаги, чтобы вернуться к предыдущей версии сервера.

Прежде чем начать

Чтобы вы смогли выполнить эту задачу, у вас должна быть полная резервная копия пула хранения, созданная до обновления до версии 8.1.5.

Об этой задаче

Используйте приведенную ниже информацию, если какое-то время у вас работал сервер V8.1.5 и вы в это время выполняли любое из следующих действий (или оба эти действия):

- Вы включили функцию дедупликации данных для любых пулов хранения, которые существовали до обновления до программы версии 8.1.5. Дедупликация данных применима только к пулам хранения, в которых используется тип устройств FILE.
- После обновления вы создали новые первичные пулы хранения *и* перенесли в эти новые пулы хранения данные, хранившиеся в других пулах хранения.

Выполните описанные ниже шаги после восстановления сервера до V7.

Процедура

- Для каждого пула хранения, для которого вы включили функцию дедупликации данных, восстановите весь пул хранения при помощи команды RESTORE STGPOOL.
- Для пулов хранения, созданных после обновления, определите, какие действия вам следует предпринять. Данные, перенесенные из существующих пулов хранения V8 в новые пулы хранения, могут быть потеряны, так как на восстановленном сервере V8 этих новых пулов не будет. Возможный способ выхода из этой ситуации зависит от типа пула хранения:
    - Если данные были перенесены в новый пул хранения из пулов хранения типа DISK, относящихся к V8, пространство, которое занимали перенесенные данные, вероятнее всего, было уже использовано повторно. Поэтому вы должны будете восстановить исходные пулы хранения V8, используя резервные копии этого пула хранения, созданные перед обновлением до V8.1.5.

      Если в новый пул хранения *не* переносились никакие данные из пулов хранения типа DISK, относящихся к V8, то произведите аудит томов пула хранения в этих пулах хранения типа DISK.

    - Если данные были перенесены в новый пул хранения из пулов хранения с последовательным доступом, относящихся к V8, эти данные могут все еще существовать на томах пула хранения на восстановленном сервере V8 и быть пригодны для использования. Эти данные, вероятнее всего, будут пригодны для использования, если для параметра REUSEDELAY для этого пула хранения было задано значение, не позволившее произвести в нем консолидацию пространства, когда сервер работал как сервер V8.1.5. Если какие-либо тома были подвергнуты консолидации, когда сервер работал как сервер Версии 8.1.5, эти тома нужно будет восстановить из резервных копий пула хранения, созданных перед обновлением до V8.1.5.

Windows: Справочная информация: Команды DB2 для баз данных сервера IBM Spectrum Protect

Используйте этот список как справочник, если служба поддержки IBM® предложит вам ввести команды DB2.

Назначение

Иногда после использования мастеров по установке и конфигурированию IBM Spectrum Protect вам потребуется ввести команды DB2. Ограниченный набор команд DB2, которые вы можете использовать (в частности, по указанию службы поддержки), представлен в списке в Табл. 1. Это не исчерпывающий список, он представлен только в виде дополнительного материала. Не предполагается, что администратор IBM Spectrum Protect будет ежедневно или вообще

регулярно использовать эти команды. Приведены примеры использования некоторых команд. Подробности выходной информации не представлены.

Полное объяснение описанных здесь команд и их синтаксиса смотрите в Информационном центре Информация о DB2.

Табл. 1. Команды DB2

Команда	**Описание**	**Пример**
Операционные системы Windows db2cmd	Операционные системы WindowsОткрывает окно инструментов командной строки DB2 и использует среду командной строки DB2.	Операционные системы Windows Открыть окно команд DB2: `db2cmd`
db2icrt	Создает экземпляры DB2 в домашнем каталоге владельца экземпляра. Совет: Мастер по конфигурированию IBM Spectrum Protect создает экземпляр, используемый сервером и базой данных. После того, как сервер установлен и сконфигурирован с помощью мастера по конфигурированию, команда db2icrt обычно не используется. Операционные системы WindowsЭта утилита расположена в каталоге DB2PATH\bin, где DB2PATH представляет собой положение установки копии DB2.	Создайте экземпляр IBM Spectrum Protect вручную.Введите команду в одной строке: `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`имя_экземпляра имя_экземпляра`*
db2set	Выводит переменные DB2.	Вывести список переменных DB2: `db2set`
CATALOG DATABASE	Сохраняет информацию о положении базы данных в системном каталоге баз данных. База данных может находиться или на локальной рабочей станции, или на удаленном сервере разделов базы данных. Мастер по конфигурированию серверов учитывает все каталоги, которые нужны для использования базы данных сервера. После того, как сервер сконфигурирован и запущен, вручную запустите эту команду, только если что-то в среде изменяется или повреждено.	Каталогизируйте базу данных: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Соединяется с заданной базой данных для использования интерфейса командной строки (command-line interface, CLI).	Соединитесь с базой данных IBM Spectrum Protect в интерфейсе командной строки DB2: `db2 connect to tsmdb1`

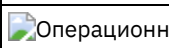
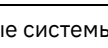
Команда	Описание	Пример

GET DATABASE CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Показать информацию конфигурации и для алиаса базы данных:
		`db2 get db cfg for tsmdb1`
		Получить информацию для проверки параметров конфигурации и базы данных, режима журналов и техобслуживания.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Возвращает значения индивидуальных записей в файле конфигурации конкретной базы данных. Важное замечание: Эти параметры и команды задаются и управляются непосредственно DB2. Они перечислены здесь в информационных целях и служат для просмотра существующих параметров. Изменение этих параметров может быть рекомендовано службой поддержки IBM или в служебных бюллетенях, таких как APAR или документы Технического руководства (technotes). Не изменяйте эти параметры вручную. Изменяйте их только по указанию службы технической поддержки IBM и только с использованием команд или процедур сервера IBM Spectrum Protect.	Получить информацию конфигурации и для менеджера баз данных: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Получает информацию о состоянии работоспособности для менеджера баз данных и его баз данных. Возвращаемая информация представляет снимок состояния работоспособности на момент ввода команды. IBM Spectrum Protect отслеживает состояние базы данных при помощи снимка работоспособности и других механизмов, представленных DB2. Может так случиться, что снимок работоспособности или другой инструмент документации DB2 свидетельствует о возможном состоянии оповещения некоторого элемента или ресурса базы данных. Это означает, что нужно принять меры для исправления ситуации. IBM Spectrum Protect отслеживает условия и отвечает соответствующим образом. Обрабатываются не все выявленные оповещения DB2.	Получить отчет об индикаторах отслеживания работоспособности DB2: `db2 get health snapshot for database on tsmdb1`

Команда	Описание	Пример

GRANT (Полномочия базы данных)	Предоставляет полномочия, применимые ко всей базе данных, в отличие от привилегий, применимых к конкретным объектам в базе данных.	Предоставить доступ для ID пользователя itmuser:
		
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Изменяет статистику, относящуюся к характеристикам таблицы и связанных индексов, или статистические производные таблицы. Эти характеристики включают в себя количество записей, количество страниц и среднюю длину записи. Запустите эту утилиту, чтобы увидеть таблицу после ее изменения или реорганизации. Производная таблица должна быть включена для оптимизации, чтобы ее можно было использовать для оптимизации запросов. Включенная для оптимизации производная таблица называется статистической производной таблицей. Используйте оператор DB2 ALTER VIEW , чтобы включить производную таблицу для оптимизации. Запустите утилиту RUNSTATS, когда изменения в рассматриваемых таблицах существенно влияют на возвращаемые в производной таблице строки. Совет: Сервер конфигурирует DB2 для запуска при необходимости команды RUNSTATS.	Изменить статистику для одной таблицы. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
	 Операционные системы WindowsОпределяет, какой экземпляр применяется к текущему сеансу.	 Операционные системы Windows Определить, какой экземпляр применим: `set db2instance=tsminst1`
SET SCHEMA	Изменяет значение специального регистра CURRENT SCHEMA, подготавливаясь к вводу команд SQL непосредственно через интерфейс командной строки DB2. Совет: Специальный регистр - это область хранения, определенная для процесса применения менеджером баз данных. Он используется для хранения информации, на которую могут ссылаться операторы SQL.	Задать схему для IBM Spectrum Protect: `db2 set schema tsmdb1`
START DATABASE MANAGER	Запускает фоновые процессы текущего экземпляра менеджера баз данных. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Запустить менеджер баз данных: `db2start`

Команда	Описание	Пример
STOP DATABASE MANAGER	Останавливает текущий экземпляр менеджера баз данных. Менеджер баз данных остается активным, пока он не остановлен явным образом. Эта команда не останавливает экземпляр менеджера баз данных, если какие-либо приложения соединены с базами данных. Если соединений с базой данных нет, но есть подключения экземпляра, эти подключения экземпляра первыми принудительно прерываются данной командой. Затем она останавливает менеджер баз данных. Перед остановкой менеджера баз данных эта команда деактивирует также все невыполненные обращения к базе данных. Для клиента эта команда недопустима. Сервер запускает и останавливает экземпляр и базу данных при всех запусках и остановках сервера. Важное замечание: Разрешить серверу управлять запуском и остановкой экземпляра и базы данных, если иное не указано службой поддержки IBM.	Остановить менеджер баз данных: `db2 stop dbm`

Windows: Деинсталляция IBM Spectrum Protect

Ниже описаны процедуры по деинсталляции IBM Spectrum Protect. Прежде чем удалять IBM Spectrum Protect, убедитесь, что вы не потеряете ваши резервные копии и архивные данные.

Прежде чем начать

Прежде чем деинсталлировать IBM Spectrum Protect, выполните следующие шаги:

- Выполните полное резервное копирование базы данных.
- Сохраните копию хронологии томов и файлов конфигурации устройств.
- Поместите полученные тома в надежное место.

 Операционные системы WindowsВнимание: Не используйте для деинсталляции IBM Spectrum Protect утилиту Установка и удаление программ в панели управления Windows. Используйте только процедуру деинсталляции, описанную в данном разделе.

Об этой задаче

IBM Spectrum Protect можно деинсталлировать любым из следующих способов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

- Windows: Деинсталляция IBM Spectrum Protect при помощи графического мастера
  IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.
- Windows: Деинсталляция IBM Spectrum Protect в режиме консоли
  Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.
- Windows: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений
  Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.
- Windows: Деинсталляция и переустановка IBM Spectrum Protect
  Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.
- Windows: Деинсталляция IBM Installation Manager
  Можно деинсталлировать IBM Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Дальнейшие действия

Информацию о том, какие шаги по установке нужно выполнить, чтобы переустановить компоненты IBM Spectrum Protect, смотрите в разделе Windows: Установка компонентов сервера.

Windows: Деинсталляция IBM Spectrum Protect при помощи графического мастера

IBM Spectrum Protect можно деинсталлировать при помощи мастера установки IBM® Installation Manager.

Процедура

1. Запустите Installation Manager.

   Операционные системы WindowsОткройте Installation Manager из меню Пуск.

2. Щелкните по Деинсталлировать.
3. Выберите Сервер IBM Spectrum Protect и щелкните по Далее.
4. Щелкните по Деинсталлировать.
5. Щелкните по Готово.

Windows: Деинсталляция IBM Spectrum Protect в режиме консоли

Чтобы деинсталлировать IBM Spectrum Protect из командной строки, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы Windowseclipse\tools

   Например:

   - Операционные системы WindowsC:\Program Files\IBM\Installation Manager\eclipse\tools
2. В каталоге tools введите следующую команду:
   - Операционные системы Windows`imcl.exe -c`
3. Для деинсталляции введите `5`.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите `N` (Next - Далее).
6. Выберите деинсталляцию пакета сервера IBM Spectrum Protect.
7. Введите `N` (Next - Далее).
8. Введите `U` (Uninstall - Деинсталляция).
9. Введите `F` (Finish - Готово).

Windows: Деинсталляция IBM Spectrum Protect в режиме без вывода сообщений

Чтобы деинсталлировать IBM Spectrum Protect в режиме без вывода сообщений, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции компонентов сервера IBM Spectrum Protect в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, uninstall_response_sample.xml, в каталоге input в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Если вы хотите деинсталлировать все компоненты IBM Spectrum Protect, оставьте заданное значение `modify="false"` для каждого компонента в файле ответов. Если вы не хотите деинсталлировать компонент, задайте значение `modify="true"`.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы Windowseclipse\tools

   Например:

   - Операционные системы WindowsC:\Program Files\IBM\Installation Manager\eclipse\tools
2. В каталоге tools введите следующую команду, где *файл_ответов* - это полное имя файла ответов:
   Операционные системы Windows

   ```
   imcl.exe -input файл_ответов -silent
   ```

   Пример команды:

   Операционные системы Windows

   ```
   imcl.exe -input C:\tmp\input\uninstall_response.xml -silent
   ```

Windows: Деинсталляция и переустановка IBM Spectrum Protect

Если вы собираетесь переустановить IBM Spectrum Protect вручную, а не пользоваться мастером, вы должны будете выполнить ряд шагов, чтобы сохранить имена экземпляров сервера и каталогов баз данных. При деинсталляции все имеющиеся у вас экземпляры сервера удаляются, но каталоги для этих экземпляров остаются.

Об этой задаче

Чтобы вручную деинсталлировать и переустановить IBM Spectrum Protect, выполните следующие шаги:

1. Операционные системы WindowsПрежде чем приступать к деинсталляции, создайте список текущих экземпляров сервера. Выполните команду:

   ```
   db2ilist
   ```

2. Введите для каждого экземпляра сервера следующую команду:
   Операционные системы Windows

   ```
   db2 attach to server1
   db2 get dbm cfg show detail
   db2 detach
   ```

   Запишите путь базы данных для каждого экземпляра.
3. Деинсталлируйте IBM Spectrum Protect. Смотрите раздел Windows: Деинсталляция IBM Spectrum Protect.

   Операционные системы WindowsПосле деинсталляции IBM Spectrum Protect выберите Панель управления > Установка и удаление программ, чтобы убедиться что компонент IBM Spectrum Protect DB2 деинсталлирован.

4. При деинсталляции любой поддерживаемой версии IBM Spectrum Protect, включая пакет исправлений, создается файл экземпляра. Файл экземпляра создается для того, чтобы помочь вам переустановить IBM Spectrum Protect. Проверьте этот файл и используйте эту информацию, когда вас попросят ввести идентификационные данные экземпляра при переустановке. При установке в режиме без вывода сообщений вы предоставляете эти идентификационные данные при помощи переменной `INSTANCE_CRED`.
   Положение файла экземпляра:
   - Операционные системы Windows`C:\ProgramData\IBM\Tivoli\TSM\instanceList.obj` в каталоге установки сервера IBM Spectrum Protect
5. Переустановите IBM Spectrum Protect. Смотрите раздел Windows: Установка компонентов сервера.

   Если файл `instanceList.obj` не существует, вы должны заново создать экземпляры сервера, используя следующие шаги:

   a. Заново создайте экземпляры сервера. Смотрите раздел Windows: Создание экземпляра сервера.
      Совет: Мастер установки сконфигурирует экземпляры сервера, но вы должны убедиться, что они существуют. Если они не существуют, вы должны будете сконфигурировать их вручную.
   b. Каталогизируйте базу данных. Поочередно войдите в систему от имени пользователя экземпляра для каждого экземпляра сервера и введите следующие команды:
      Операционные системы Windows

```
set db2instance=server1
db2 catalog database tsmdb1
db2 attach to server1
db2 update dbm cfg using dftdbpath диск_экземпляра
db2 detach
```

c. Убедитесь, что IBM Spectrum Protect распознает экземпляры сервера, вызвав спи сок ваших каталогов. Вы увидите ваш домашний каталог (если вы его не изменили). Если вы использовали мастер конфигурирования, ваш каталог экземпляра не появится. Введите команду:

```
db2 list database directory
```

Если вы увидите в списке TSMDB1, вы можете запустить сервер.

Windows: Деинсталляция IBM Installation Manager

Можно деинсталлировать IBM® Installation Manager, если у вас больше нет продуктов, установленных IBM Installation Manager.

Прежде чем начать

Перед удалением IBM Installation Manager, необходимо убедиться, что все пакеты, установленные IBM Installation Manager, удалены. Закройте IBM Installation Manager перед запуском деинсталляции.

Операционные системы WindowsДля просмотра установленных пакетов щелкните по Запуск > Все программы > IBM Installation Manager > Показать установленные пакеты.

Процедура

Чтобы деинсталлировать IBM Installation Manager, выполните следующие шаги:

Операционные системы Windows

1. В меню Пуск щелкните по Панель управления > Программы и компоненты.
2. Выберите IBM Installation Manager и щелкните Деинсталляция.

Обновление до V8.1

Чтобы воспользоваться преимуществами новых функций и обновлений продукта, обновите сервер IBM Spectrum Protect до версии 8.1.5.

Об этой задаче

Чтобы обновить сервер в той же операционной системе, смотрите инструкции по обновлению. Инструкции по перенастройке сервера в другую операционную систему смотрите в документе Процесс перенастройки и обновления IBM Spectrum Protect - Часто задаваемые вопросы.

Табл. 1. Инструкции по обновлению

Для обновления от версии	**До версии**	**Смотрите следующую информацию**
V8.1	V8.1 с пакетом исправлений V8.1 или промежуточным исправлением	Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect
V7.1	V8.1	Установка сервера и проверка обновления

Для обновления от версии	До версии	Смотрите следующую информацию
V7.1	V8.1 с пакетом исправлений V8.1 или промежуточным исправлением	 Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect  Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect  Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect
V5.5, V6.2 или V6.3	V8.1	IBM Spectrum Protect Процесс обновления и перенастройки - Часто задаваемые вопросы

Обновление версии 7 до версии 8.1 занимает примерно 20-50 минут. Результаты в вашей среде могут отличаться от результатов, полученных в лабораториях.

Информацию об обновлении в кластерной среде смотрите в разделе Обновление сервера в кластерной среде.

Чтобы вернуться к прежней версии сервера после обновления или перенастройки, вам потребуется полная резервная копия базы данных и программа установки для исходной версии сервера. У вас также должны быть следующие важнейшие файлы конфигурации:

- Файл хронологии тома
- Файл конфигурации устройств
- Файл серверных опций

- Обновление до V8.1
  Сервер можно обновить непосредственно с V7.1 до V8.1. Деинсталировать V7.1 не нужно.
- Обновление сервера в кластерной среде
  Чтобы обновить сервер до версии 8.1.5 в кластерной среде, нужно выполнить задачи подготовки и установки. Эти процедуры зависят от операционной системы и выпуска.

Информация, связанная с данной:
Процесс обновления и перенастройки IBM Spectrum Protect - Часто задаваемые вопросы

Обновление до V8.1

Сервер можно обновить непосредственно с V7.1 до V8.1. Деинсталировать V7.1 не нужно.

Прежде чем начать

Убедитесь, что вы сохранили носитель установки базового выпуска сервера, который вы обновляете. Если вы устанавливали компоненты сервера с DVD-диска, то убедитесь, что этот DVD-диск доступен. Если вы устанавливали компоненты сервера из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет при этом деинсталлирован, то носитель установки базового выпуска сервера понадобится, чтобы переустановить лицензию.
Совет: Для V8.1 и новее DVD-диски больше не поставляются.

Процедура

Чтобы обновить сервер до V8.1, выполните следующие задачи:

- Планирование обновления
  Перед обновлением сервера с V7.1 до V8.1 необходимо ознакомиться с соответствующей информацией о планировании, например, с требованиями к системе и замечаниями по выпуску. Затем, чтобы свести к минимуму влияние обновления на производственный процесс, выберите для обновления подходящие дату и время.

- Подготовка системы
  Чтобы подготовить систему к обновлению с V7.1 до V8.1, нужно собрать информацию о каждом экземпляре DB2. Затем создайте резервную копию базы данных сервера, сохраните ключевые файлы конфигурации, отмените сеансы и остановите сервер.
- Установка сервера и проверка обновления
  Чтобы завершить процесс обновления сервера до V8.1, необходимо установить сервер V8.1. Затем убедитесь, что обновление прошло успешно, запустив экземпляр сервера.

Планирование обновления

Перед обновлением сервера с V7.1 до V8.1 необходимо ознакомиться с соответствующей информацией о планировании, например, с требованиями к системе и замечаниями по выпуску. Затем, чтобы свести к минимуму влияние обновления на производственный процесс, выберите для обновления подходящие дату и время.

Об этой задаче

В лабораторных тестах процесс обновления сервера V7.1 до V8.1 занимал от 14 до 45 минут. Ваши результаты могут отличаться, в зависимости от вашей аппаратной и программной среды и от размера базы данных сервера.

Процедура

1. Ознакомьтесь с аппаратными и программными требованиями:

   Операционные системы AIXТребования для систем AIX

   Операционные системы LinuxТребования для систем Linux

   Операционные системы WindowsТребования для систем Windows

   Информацию о последних изменениях требований к системе смотрите на сайте поддержки IBM Spectrum Protect в техническом замечании 1243309.

2. Особые инструкции или особую информацию для вашей операционной системы смотрите в документе Замечания по выпуску для компонентов сервера версии 8.1 и в файлах readme для пакетов исправлений сервера IBM Spectrum Protect версии 8.1.
3. Чтобы свести к минимуму влияние обновления на производственный процесс, выберите для обновления подходящие дату и время. Время, которое требуется для обновления системы, зависит от размера базы данных и многих других факторов. При запуске процесса обновления клиенты не смогут соединиться с сервером, пока не будет установлена новая версия и не будут снова зарегистрированы все необходимые лицензии.
4. Если вы выполняете обновление сервера версии 6 или 7 до версии 8.1, убедитесь, что у вас есть системные ID и пароль для экземпляра DB2 сервера IBM Spectrum Protect. Эти учетные данные необходимы для обновления системы.

Подготовка системы

Чтобы подготовить систему к обновлению с V7.1 до V8.1, нужно собрать информацию о каждом экземпляре DB2. Затем создайте резервную копию базы данных сервера, сохраните ключевые файлы конфигурации, отмените сеансы и остановите сервер.

Процедура

1. Войдите в систему на компьютере, где установлен сервер.

   Операционные системы AIXОперационные системы LinuxПроверьте, что вы вошли в систему под ID пользователя экземпляра.

   Операционные системы WindowsПроверьте, что вы вошли в систему под ID пользователя администратора, который использовался для установки сервера V7.1.

2. Получите список экземпляров DB2. Например, введите следующую команду системы:

   Операционные системы AIXОперационные системы Linux

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

Операционные системы Windows

```
db2ilist
```

Результат выполнения команды может выглядеть, как в следующем примере:

Операционные системы AIXОперационные системы Linux

```
tsminst1
```

Операционные системы Windows

```
SERVER1
```

Убедитесь, что каждый экземпляр соответствует серверу, запущенному в этой системе.

3. Операционные системы AIXОперационные системы LinuxДля каждого экземпляра DB2 запишите каталог базы данных по умолчанию, фактический каталог базы данных, имя базы данных, алиас базы данных и все переменные DB2, сконфигурированные для этого экземпляра. Сохраните запись, так как она может понадобиться. Эти сведения нужны для восстановления базы данных V7.1.
4. Операционные системы WindowsСоберите информацию о каждом экземпляре DB2. Запишите каталог базы данных по умолчанию, фактический каталог базы данных, имя базы данных, алиас базы данных и все переменные DB2, сконфигурированные для этого экземпляра. Сохраните запись, так как она может понадобиться. Эти сведения нужны для восстановления базы данных V7.1.
   a. Откройте окно команд DB2, введя следующую системную команду:

      ```
      db2cmd
      ```

   b. Для изменения экземпляра введите следующую системную команду:

      ```
      set DB2INSTANCE=экземпляр
      ```

      где *экземпляр* указывает экземпляр DB2.
   c. Получите путь к базе данных по умолчанию для экземпляра DB2, введя следующую системную команду:

      ```
      db2 get dbm cfg | findstr DFTDBPATH
      ```

      Результат выполнения команды может выглядеть, как в следующем примере:

      ```
      Default database path                       (DFTDBPATH) = D:
      ```

   d. Получите информацию о базах данных экземпляра DB2, введя следующую системную команду:

      ```
      db2 list database directory
      ```

      Результат выполнения команды может выглядеть, как в следующем примере:

      ```
      System Database Directory

                      Number of entries in the directory = 2

                     Database 1 entry:

                      Database alias                       = TSMAL001
                      Database name                        = TSMDB1
                      Node name                            = TSMNODE1
                      Database release level               = d.00
                      Comment                              = TSM SERVER DATABASE VIA TCPIP
                      Directory entry type                 = Remote
                      Catalog database partition number    = -1
                      Alternate сервер hostname            =
                      Alternate сервер port number         =

                     Database 2 entry:

                      Database alias                       = TSMDB1
                      Database name                        = TSMDB1
                      Local database directory             = D:
                      Database release level               = d.00
                      Comment                              =
                      Directory entry type                 = Indirect
      ```

```
Catalog database partition number    = 0
Alternate сервер hostname            =
Alternate сервер port number         =
```

e. Получите переменные экземпляра DB2, введя следующую системную команду:

```
db2set -all
```

Результат выполнения команды может выглядеть, как в следующем примере:

```
[e] DB2CODEPAGE=1208
[e] DB2PATH=D:\TSM\db2
[i] DB2_PMODEL_SETTINGS=MAX_BACKGROUND_SYSAPPS:500
[i] DB2_SKIPINSERTED=ON
[i] DB2_KEEPTABLELOCK=OFF
[i] DB2_EVALUNCOMMITTED=ON
[i] DB2_VENDOR_INI=D:\Server1\tsmdbmgr.env
[i] DB2_SKIPDELETED=ON
[i] DB2INSTPROF=C:\ProgramData\IBM\DB2\DB2TSM1
[i] DB2COMM=TCPIP
[i] DB2CODEPAGE=819
[i] DB2_PARALLEL_IO=*
[g] DB2_EXTSECURITY=YES
[g] DB2_COMMON_APP_DATA_PATH=C:\ProgramData

[g] DB2PATH=D:\TSM\db2
[g] DB2INSTDEF=SERVER1
```

5. Соединитесь с сервером, указав ID пользователя-администратора.
6. Создайте резервную копию базы данных при помощи команды BACKUP DB. Рекомендуется использовать резервное копирование в режиме снимка, которое создает полную резервную копию базы данных без прерывания запланированного резервного копирования. Например, можно создать резервную копию снимка, введя следующую команду администрирования:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

7. Создайте в другом каталоге резервную копию информации о конфигурации устройств при помощи следующей команды администрирования:

   ```
   backup devconfig filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
   Совет: Этот файл потребуется, если вы решите восстановить базу данных V7.1.
8. Скопируйте файл хронологии томов в другой каталог. Введите следующую команду администрирования:

   ```
   backup volhistory filenames=имя_файла
   ```

   где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
   Совет: Этот файл потребуется, если вы решите восстановить базу данных V7.1.
9. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt. Этот файл расположен в каталоге экземпляра сервера.
10. Запретите операции на сервере, отключив новые сеансы. Введите следующие административные команды:

    ```
    disable sessions client
    disable sessions server
    ```

11. Проверьте, существуют ли какие-либо сеансы, и сообщите пользователям, что сервер будет остановлен. Чтобы проверить наличие существующих сеансов, введите команду администрирования:

    ```
    query session
    ```

12. Отмените сеансы, введя следующую команду администрирования:

    ```
    cancel session all
    ```

    Эта команда отменяет все сеансы, кроме вашего текущего сеанса.
13. Остановите сервер, введя следующую команду администрирования:

    ```
    halt
    ```

14. Убедитесь, что сервер завершил работу и никакие процессы не выполняются.

Операционные системы AIXОперационные системы LinuxВведите следующую команду:

```
ps -ef | grep dsmserv
```

Операционные системы WindowsОткройте приложение Диспетчер задач Windows и просмотрите список активных процессов.

15. В каталоге экземпляра сервера вашей установки найдите файл NODELOCK и переместите его в другой каталог, где вы сохраняете файлы конфигурации. Файл NODELOCK содержит сведения об использованных лицензиях для вашей установки. Эта информация о лицензиях заменяется при выполнении обновления.

Ссылки, связанные с данной:
BACKUP DB (Выполнить резервное копирование базы данных)
Команда BACKUP DEVCONFIG (создание резервных копий информации о конфигурации устройства)
BACKUP VOLHISTORY (сохранение информации хронологии томов с последовательным доступом)
DISABLE SESSIONS (Запретить новым сеансам доступ к Tivoli Storage Manager)
QUERY SESSION (запрос информации о клиентских сеансах)
CANCEL SESSION (отмена одного или нескольких клиентских сеансов)
HALT (выключение сервера)

Установка сервера и проверка обновления

Чтобы завершить процесс обновления сервера до V8.1, необходимо установить сервер V8.1. Затем убедитесь, что обновление прошло успешно, запустив экземпляр сервера.

Прежде чем начать

Операционные системы AIXОперационные системы LinuxВы должны быть зарегистрированы в системе под ID пользователя root.

Операционные системы WindowsНужно войти в систему с ID администратора, который использовался при установке предыдущего сервера.

Пакет установки можно получить с сайта скачивания IBM®.

Операционные системы AIXОперационные системы LinuxЗадайте предел максимального размера файла для системного пользователя, чтобы убедиться, что файлы можно успешно скачать.

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

   ```
   ulimit -Hf
   ```

2. Если предельный максимальный размер файла для системного пользователя не задан как неограниченный, измените параметр на неограниченный, выполнив инструкции в документации для вашей операционной системы.

Об этой задаче

При помощи программы установки IBM Spectrum Protect можно установить следующие компоненты:

- Сервер
  Совет: База данных (DB2), Global Security Kit (GSKit) и IBM Java™ Runtime Environment (JRE) автоматически устанавливаются при выборе компонента сервера.
- Языки сервера
- Лицензия
- Устройства
- IBM Spectrum Protect for SAN
- Центр операций

Процедура

1. Скачайте соответствующий файл пакета с одного из следующих веб-сайтов:
   - Скачайте пакет сервера со страницы Passport Advantage или Fix Central.
   - Самую последнюю информацию, обновления и исправления обслуживания смотрите в разделе Портал поддержки IBM.

2. Сделайте следующее:

Операционные системы AIXОперационные системы Linux
Операционные системы AIXОперационные системы Linux
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к пространству смотрите в документе по скачиванию для вашего продукта.
      - IBM Spectrum Protect техническое замечание 4042944
      - IBM Spectrum Protect Extended Edition техническое замечание 4042945
      - IBM Spectrum Protect for Data Retention техническое замечание 4042946
   b. Скачайте файл пакета в каталог по вашему выбору. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.

      Кроме того, у вас должны быть разрешения на запуск выполняемых файлов для файла пакета.

   c. Если потребуется, введите следующую команду, чтобы изменить разрешения на доступ к файлам:

      ```
      chmod a+x имя_пакета.bin
      ```

      где *имя_пакета* выглядит как в следующем примере:

      Операционные системы AIX

      ```
      8.1.x.000-IBM-SPSRV-AIX.bin
      ```

      Операционные системы Linux

      ```
      8.1.x.000-IBM-SPSRV-Linuxs390x.bin
      8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
      8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
      ```

      В примерах *8.1.x.000* представляет уровень выпуска продукта.
   d. Извлеките файлы установки, введя следующую команду:

      ```
      ./имя_пакета.bin
      ```

      Это большой пакет. Поэтому извлечение файлов займет некоторое время.

Операционные системы Windows
Операционные системы Windows
   a. Убедитесь, что у вас будет достаточно места для хранения файлов установки, когда они будут извлечены из пакета продукта. Требования к пространству смотрите в документе по скачиванию для вашего продукта.
      - IBM Spectrum Protect техническое замечание 4042944
      - IBM Spectrum Protect Extended Edition техническое замечание 4042945
      - IBM Spectrum Protect for Data Retention техническое замечание 4042946
   b. Перейдите в каталог, куда вы поместили исполняемый файл.
      Совет: В следующем шаге файлы извлекаются в текущий каталог. Имя каталога может содержать не более 128 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.
   c. Для извлечения файлов установки дважды щелкните по исполняемому файлу:

      ```
      имя_пакета.exe
      ```

      Где *имя_пакета* аналогично следующему примеру:

      ```
      8.1.x.000-SPSRV-WindowsX64.exe
      ```

      Это большой пакет. Поэтому извлечение файлов займет некоторое время.

3. Операционные системы AIXДля правильной работы мастеров IBM Spectrum Protect должна быть разрешена команда `lsuser`.
4. Установите программное обеспечение IBM Spectrum Protect одним из следующих способов. Установите лицензию на IBM Spectrum Protect в процессе установки.
   Совет: Если в системе используется несколько экземпляров сервера, установите программу IBM Spectrum Protect только один раз, чтобы обновить все экземпляры сервера.

   Мастер установки

Операционные системы AIXЧтобы установить сервер при помощи графического мастера IBM Installation Manager, выполните инструкции из раздела Установка IBM Spectrum Protect при помощи мастера установки.

Операционные системы LinuxЧтобы установить сервер при помощи графического мастера IBM Installation Manager, выполните инструкции из раздела Установка IBM Spectrum Protect при помощи мастера установки.

Операционные системы WindowsЧтобы установить сервер при помощи графического мастера IBM Installation Manager, выполните инструкции из раздела Установка IBM Spectrum Protect при помощи мастера установки.

Убедитесь, что система соответствует обязательным требованиям для использования мастера установки. Затем выполните процедуру установки. В окне IBM Installation Manager щелкните по значку Обновить или Изменить.

Установка сервера с использованием режима консоли

Операционные системы AIXЧтобы установить сервер в режиме консоли, следуйте инструкциям в разделе УстановкаTivoli Storage Manager в режиме консоли.

Операционные системы LinuxЧтобы установить сервер в режиме консоли, следуйте инструкциям в разделе УстановкаTivoli Storage Manager в режиме консоли.

Операционные системы WindowsЧтобы установить сервер в режиме консоли, следуйте инструкциям в разделе УстановкаTivoli Storage Manager в режиме консоли.

Ознакомьтесь с информацией об установке сервера в режиме консоли и затем выполните процедуру установки.

Режим без вывода сообщений

Операционные системы AIXЧтобы установить сервер в режиме без вывода сообщений, выполните инструкции из раздела Установка Tivoli Storage Manager в режиме без вывода сообщений.

Операционные системы LinuxЧтобы установить сервер в режиме без вывода сообщений, выполните инструкции из раздела Установка Tivoli Storage Manager в режиме без вывода сообщений.

Операционные системы WindowsЧтобы установить сервер в режиме без вывода сообщений, выполните инструкции из раздела Установка Tivoli Storage Manager в режиме без вывода сообщений.

Ознакомьтесь с информацией об установке сервера в режиме без вывода сообщений и затем выполните процедуру установки.

После установки программы переконфигурировать систему не нужно.

5. Исправьте ошибки, обнаруженные в процессе установки.

   Если вы установили сервер с использованием мастера установки, то вы можете посмотреть журналы установки при помощи инструмента IBM Installation Manager. Щелкните по Файл > Просмотреть журнал. Чтобы собрать файлы журналов, щелкните в IBM Installation Manager по Справка > Экспорт данных для анализа ошибок.

   Если вы установили сервер в режиме консоли или в режиме без вывода сообщений, то вы можете просмотреть журналы ошибок в каталоге журнала IBM Installation Manager, например:
   - Операционные системы AIXОперационные системы Linux/var/ibm/InstallationManager/logs
   - Операционные системы WindowsC:\ProgramData\IBM\Installation Manager\logs
6. Перейдите в раздел Портал поддержки IBM, чтобы получить исправления. Щелкните по Fixes, updates, and drivers (Исправления, обновления и драйверы) и примените все необходимые исправления.
7. Проверьте, успешно ли выполнено обновление:
   a. Запустите экземпляр сервера.

      Операционные системы AIXИнструкции смотрите в разделе Запуск экземпляра сервера.

      Операционные системы LinuxИнструкции смотрите в разделе Запуск экземпляра сервера.

   b. Следите за сообщениями, которые сервер генерирует при запуске. Следите за сообщениями об ошибках и предупреждениями и разрешите соответствующие проблемы.
   c. Проверьте, можете ли вы соединиться с сервером с помощью клиента администрирования. Для запуска сеанса клиента администрирования введите следующую команду администрирования IBM Spectrum Protect:

```
dsmadmc
```

d. Запустите команды QUERY для получения информации об обновленной системе. Например, чтобы получить объединенную информацию о системе, введите следующую команду администрирования IBM Spectrum Protect:

```
query system
```

Для получения информации о базе данных введите следующую команду администрирования IBM Spectrum Protect:

```
query db format=detailed
```

8.  Операционные системы WindowsПроверьте, успешно ли выполнено обновление:
   a. Запустите экземпляр сервера. Для запуска сервера из каталога по умолчанию C:\Program Files\Tivoli\TSM введите следующую команду администрирования IBM Spectrum Protect:

   ```
   dsmserv -k экземпляр_сервера
   ```

   экземпляр_сервера - это имя вашего экземпляра сервера. По умолчанию, именем первого экземпляра сервера IBM Spectrum Protect является Server1.

   Если вы планируете запустить сервер как службу в учетной записи локальной системы, этот учетной записи должен быть явно предоставлен доступ к базе данных сервера. Инструкции смотрите в разделе Запуск сервера с использованием служб Windows.

   b. Следите за сообщениями, которые сервер генерирует при запуске. Следите за сообщениями об ошибках и предупреждениями и разрешите соответствующие проблемы.
   c. Проверьте, можете ли вы соединиться с сервером с помощью клиента администрирования. Для запуска сеанса клиента администрирования введите следующую команду администрирования IBM Spectrum Protect:

   ```
   dsmadmc
   ```

   d. Запустите команды QUERY для получения информации об обновленной системе. Например, чтобы получить объединенную информацию о системе, введите следующую команду администрирования IBM Spectrum Protect:

   ```
   query system
   ```

   Для получения информации о базе данных введите следующую команду администрирования IBM Spectrum Protect:

   ```
   query db format=detailed
   ```

9.  Операционные системы AIX  Операционные системы LinuxЗарегистрируйте лицензии для установленных в вашей системе компонентов сервера IBM Spectrum Protect, введя команду REGISTER LICENSE:

   ```
   register license file=каталог_установки/server/bin/имя_компонента.lic
   ```

   где *каталог_установки* указывает каталог, в который вы установили компонент, а *имя_компонента* указывает аббревиатуру для этого компонента.

   Например, если вы установили сервер в каталоге по умолчанию /opt/tivoli/tsm, введите следующую команду, чтобы зарегистрировать лицензию:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
   ```

   Например, если вы установили IBM Spectrum Protect Extended Edition в каталог /opt/tivoli/tsm, введите следующую команду:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
   ```

   Например, если вы установили IBM Spectrum Protect for Data Retention в каталог /opt/tivoli/tsm, введите следующую команду:

   ```
   register license file=/opt/tivoli/tsm/server/bin/dataret.lic
   ```

   Ограничение:
   Вы не можете использовать сервер IBM Spectrum Protect для регистрации лицензий на следующие продукты:
   - IBM Spectrum Protect for Mail

- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Команда REGISTER LICENSE не применяется к этим лицензиям. Лицензирование этих продуктов выполняется клиентами IBM Spectrum Protect.

10. Операционные системы WindowsЗарегистрируйте лицензии для установленных в вашей системе компонентов сервера, введя команду REGISTER LICENSE:

    ```
    register license file=каталог_установки\server\имя_компонента.lic
    ```

    Где *каталог_установки* указывает каталог, в который вы установили компонент, а *имя_компонента* указывает аббревиатуру для этого компонента.

    Например, если вы установили сервер в каталоге по умолчанию, c:\Program Files\Tivoli\TSM, введите следующую команду, чтобы зарегистрировать лицензию:

    ```
    register license file=c:\Program Files\Tivoli\TSM\server\tsmbasic.lic
    ```

    Например, если вы установили IBM Spectrum Protect Extended Edition в каталог c:\Program Files\Tivoli\TSM, то введите следующую команду:

    ```
    register license file=c:\Program Files\Tivoli\TSM\server\tsmee.lic
    ```

    Например, если вы установили IBM Spectrum Protect for Data Retention в каталог c:\Program Files\Tivoli\TSM, то введите следующую команду:

    ```
    register license file=c:\Program Files\Tivoli\TSM\server\dataret.lic
    ```

    Ограничение:
    Вы не можете использовать сервер IBM Spectrum Protect для регистрации лицензий на следующие продукты:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Команда REGISTER LICENSE не применяется к этим лицензиям. Лицензирование этих продуктов выполняется клиентами IBM Spectrum Protect.
11. Необязательно: Для установки дополнительного пакета поддержки национального языка используйте функцию изменения IBM Installation Manager.
12. Необязательно: Для обновления языкового пакета до более новой версии используйте функцию обновления IBM Installation Manager.

Дальнейшие действия

Пароли можно аутентифицировать с помощью сервера каталогов LDAP или сервера IBM Spectrum Protect. Пароли, которые аутентифицированы с помощью сервера каталогов LDAP, могут обеспечить расширенную защиту системы.

Операционные системы WindowsЕсли в Windows есть драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, используйте этот драйвер устройств. Если в Windows нет драйвера для ленточных устройств или чейнджеров, которыми вы намерены воспользоваться, установите драйвер IBM Spectrum Protect, введя команду `dpinst.exe /a`. Файл `dpinst.exe` находится в каталоге драйверов устройств. Каталог по умолчанию - C:\Program Files\Tivoli\TSM\device\drivers.

Ссылки, связанные с данной:
QUERY SYSTEM (получение данных о конфигурации и емкости системы)
QUERY DB (просмотр информации о базе данных)
REGISTER LICENSE (регистрация новой лицензии)
Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Обновление сервера в кластерной среде

Чтобы обновить сервер до версии 8.1.5 в кластерной среде, нужно выполнить задачи подготовки и установки. Эти процедуры зависят от операционной системы и выпуска.

Процедура

Выполните процедуру для используемой операционной системы, исходной версии и версии назначения:

Операционные системы AIX

Табл. 1. Процедуры по обновлению сервера в кластерной среде в операционной системе AIX

Исходный выпуск	Выпуск назначения	Процедура
V8.1	Пакет исправлений V8.1.5	Применение пакета исправлений к V8 в кластерной среде для AIX
V6.3 или V7.1	V8.1.5	Обновление IBM Spectrum Protect версии 6.3 или V7.1 до версии 8.1.5 в кластерной среде для AIX с совместно используемым экземпляром базы данных Обновление версии 6.3 до версии 8.1.5 в кластерной среде для AIX с отдельными экземплярами базы данных
V5.5, V6.1, V6.2	Версия 7.1.1 или более поздняя	IBM Spectrum Protect Процесс обновления и перенастройки - Часто задаваемые вопросы

Операционные системы Linux

Табл. 2. Процедуры по обновлению сервера в кластерной среде в операционной системе Linux

Исходный выпуск	Выпуск назначения	Процедура
Версия 6.3 или более поздняя	V8.1.5	Обновление сервера, сконфигурированного с использованием System Automation for Multiplatforms

Операционные системы Windows

Табл. 3. Процедуры по обновлению сервера в кластерной среде в операционной системе Windows

Исходный выпуск	Выпуск назначения	Процедура
V8.1	Пакет исправлений V8.1.5	Применение пакета исправлений к V8 в кластерной среде для Windows
V6.3 или V7.1	V8.1.5	Обновление V6.3 или V7.1 до V8.1 в кластерной среде в Windows
V5.5, V6.1, V6.2	Версия 7.1 или более поздняя	IBM Spectrum Protect Процесс обновления и перенастройки - Часто задаваемые вопросы

- Обновление IBM Spectrum Protect версии 6.3 или V7.1 до версии 8.1.5 в кластерной среде для AIX с совместно используемым экземпляром базы данных
  Сервер IBM Spectrum Protect версии 6.3 или версии 7.1 можно обновить до версии 8.1.5 в кластерной среде AIX с совместно используемым экземпляром базы данных. После этого вы сможете использовать новые функции IBM Spectrum Protect версии 8.1.5.
- Обновление версии 6.3 до версии 8.1.5 в кластерной среде для AIX с отдельными экземплярами базы данных
  Можно обновить сервер версии 6.3 до версии 8.1.5 в кластерной среде AIX с отдельными экземплярами базы данных. После этого вы сможете использовать новые функции версии 8.1.5.
- Обновление IBM Spectrum Protect до версии 8.1.5 в кластерной среде для Linux
  Для использования новых функций IBM Spectrum Protect можно обновить сервер IBM Spectrum Protect, установленный в Linux в кластерной среде.
- Обновление сервера V6.3 или V7.1 до V8.1.5 в кластерной среде для Windows
  Для использования новых функций продукта можно обновить сервер, установленный в операционной системе Windows в кластерной среде, с версии 6 или 7.1 до IBM Spectrum Protect версии 8.1.5.

Операционные системы AIX

Обновление IBM Spectrum Protect версии 6.3 или V7.1 до версии 8.1.5 в кластерной среде для AIX с совместно используемым экземпляром базы данных

Сервер IBM Spectrum Protect версии 6.3 или версии 7.1 можно обновить до версии 8.1.5 в кластерной среде AIX с совместно используемым экземпляром базы данных. После этого вы сможете использовать новые функции IBM Spectrum Protect версии 8.1.5.

Прежде чем начать

Убедитесь, что вы сохранили носитель установки базового выпуска сервера V6.3 или V7.1, который вы обновляете. Если вы устанавливали IBM Spectrum Protect с DVD-диска, то убедитесь, что этот DVD-диск доступен. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет деинсталлирован, вы должны будете переустановить лицензию с носителя установки базового выпуска сервера.

Об этой задаче

Используйте следующую процедуру, если каталог экземпляра DB2 совместно используется узлами кластера. Каталог экземпляра DB2 находится в следующем положении:

```
/home/tsminst1/sqllib
```

Если каталог экземпляра DB2 не используется узлами совместно, следуйте инструкциям в разделе Обновление версии 6.3 до версии 8.1.5 в кластерной среде для AIX с отдельными экземплярами базы данных.

Процедура

1. Создайте резервную копию базы данных при помощи команды BACKUP DB. Рекомендуется использовать резервное копирование в режиме снимка, которое создает полную резервную копию базы данных без прерывания запланированного резервного копирования. Например, можно создать резервную копию снимка, введя следующую команду администрирования:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте в другом каталоге резервную копию информации о конфигурации устройств, введя следующую команду:

   ```
   backup devconfig filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
3. Создайте в другом каталоге резервную копию файла хронологии томов, введя следующую команду:

   ```
   backup volhistory filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt и находящегося в каталоге экземпляра сервера.
5. Остановите все экземпляры сервера. Убедитесь в отсутствии запущенных серверных процессов. Если вы используете мониторинг на уровне приложений для сервера IBM Spectrum Protect, то приостановите мониторинг ресурса приложения dsmserv при помощи инструмента кластеризации.
6. Убедитесь, что менеджер баз данных не работает не на одном экземпляре. Определите, выполняются ли процессы db2sysc. Владелец выполняемых процессов указывает, какие экземпляры активны. Для каждого владельца экземпляра сервера введите следующую команду, чтобы остановить DB2:

   ```
   db2stop
   ```

7. На основном узле установите сервер IBM Spectrum Protect V8.1.5, запустив команду ./install.sh. Инструкции смотрите в разделе Установка компонентов сервера. Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить или Изменить.
8. Запустите каждый сервер версии 8.1.5 в режиме активного окна:
   a. Убедитесь, что вы вошли в систему с ID владельца экземпляра.
   b. Перейдите в каталог экземпляра и введите следующую команду:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Подождите, пока вы не увидите сообщение сервера о том, что сервер запущен.

9. Остановите сервер для каждого обновляемого экземпляра IBM Spectrum Protect. Введите следующую команду:

   ```
   halt
   ```

   Совет: Если каталог экземпляра DB2 совместно используется узлами в кластере, перемещать совместно используемые ресурсы на вторичный узел в кластере не нужно.
10. На каждом дополнительном узле в кластере выполните следующие действия:

a. Установите сервер IBM Spectrum Protect версии 8.1.5, запустив команду ./install.sh. Инструкции смотрите в разделе Установка компонентов сервера. 8.1.
   i. Если вы используете мастер установки, щелкните в окне IBM Installation Manager по значку Обновить или Изменить.
   ii. Если вы используете мастер установки, то отмените в панели Идентификационные данные экземпляра выбор переключателя Обновить этот экземпляр для каждого экземпляра.
   iii. Если вы устанавливаете сервер в режиме консоли, то в ответ на запрос `Обновить этот экземпляр?` введите `NO` (Нет) для каждого экземпляра.
   iv. Если вы устанавливаете сервер в режиме без выдачи сообщений, то укажите `FALSE`в качестве значения переменной `user.`*`имя_экземпляра`*`_update` для каждого экземпляра.
b. Запустите все серверы IBM Spectrum Protect версии 8.1.5. Если вы используете мониторинг на уровне приложений, то запустите сервер при помощи инструмента кластеризации.

   Инструкции по запуску сервера смотрите в разделе Запуск экземпляра сервера.

11. Зарегистрируйте лицензии для установленных в вашей системе компонентов сервера, введя команду REGISTER LICENSE:

    ```
    register license file=каталог_установки/server/bin/имя_компонента.lic
    ```

    Где *каталог_установки* указывает каталог, в который вы установили компонент, а *имя_компонента* указывает аббревиатуру для этого компонента.

    Например, если вы установили сервер в каталоге по умолчанию /opt/tivoli/tsm, введите следующую команду, чтобы зарегистрировать лицензию:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
    ```

    Например, если вы установили IBM Spectrum Protect Extended Edition в каталог /opt/tivoli/tsm, введите следующую команду:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
    ```

    Например, если вы установили IBM Spectrum Protect for Data Retention в каталог /opt/tivoli/tsm, введите следующую команду:

    ```
    register license file=/opt/tivoli/tsm/server/bin/dataret.lic
    ```

    Ограничение:
    Вы не можете использовать сервер IBM Spectrum Protect для регистрации лицензий на следующие продукты:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Команда REGISTER LICENSE не применяется к этим лицензиям. Лицензирование этих продуктов выполняется клиентами IBM Spectrum Protect.

Ссылки, связанные с данной:
BACKUP DB (Выполнить резервное копирование базы данных)
Команда BACKUP DEVCONFIG (создание резервных копий информации о конфигурации устройства)
BACKUP VOLHISTORY (сохранение информации хронологии томов с последовательным доступом)
HALT (выключение сервера)
REGISTER LICENSE (регистрация новой лицензии)
Операционные системы AIX

Обновление версии 6.3 до версии 8.1.5 в кластерной среде для AIX с отдельными экземплярами базы данных

Можно обновить сервер версии 6.3 до версии 8.1.5 в кластерной среде AIX с отдельными экземплярами базы данных. После этого вы сможете использовать новые функции версии 8.1.5.

Прежде чем начать

Убедитесь, что вы сохранили носитель установки базового выпуска сервера V6.3 или V7.1, который вы обновляете. Если вы устанавливали IBM Spectrum Protect с DVD-диска, то убедитесь, что этот DVD-диск доступен. Если вы устанавливали IBM Spectrum Protect из скачанного пакета, то убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет деинсталлирован, вы должны будете переустановить лицензию с носителя установки базового выпуска сервера.

Об этой задаче

Используйте следующую процедуру, когда каталог экземпляра DB2 не используется совместно узлами кластера. Каталог экземпляра DB2 находится в следующем положении:

```
/home/tsminst1/sqllib
```

Если каталог экземпляра DB2 совместно используется узлами кластера, следуйте инструкциям в разделе Обновление IBM Spectrum Protect версии 6.3 или V7.1 до версии 8.1.5 в кластерной среде для AIX с совместно используемым экземпляром базы данных.

Процедура

1. Создайте резервную копию базы данных при помощи команды BACKUP DB. Рекомендуется использовать резервное копирование в режиме снимка, которое создает полную резервную копию базы данных без прерывания запланированного резервного копирования. Например, можно создать резервную копию снимка, введя следующую команду администрирования:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте в другом каталоге резервную копию информации о конфигурации устройств, введя следующую команду:

   ```
   backup devconfig filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
3. Создайте в другом каталоге резервную копию файла хронологии томов, введя следующую команду:

   ```
   backup volhistory filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt и находящегося в каталоге экземпляра сервера.
5. Остановите все экземпляры сервера. Убедитесь в отсутствии запущенных серверных процессов. Если вы используете мониторинг на уровне приложений для сервера IBM Spectrum Protect, то приостановите мониторинг ресурса приложения dsmserv при помощи инструмента кластеризации.
6. Убедитесь, что менеджер баз данных не работает не на одном экземпляре. Определите, выполняются ли процессы db2sysc. Владелец выполняемых процессов указывает, какие экземпляры активны. Для каждого владельца экземпляра сервера введите следующую команду, чтобы остановить DB2:

   ```
   db2stop
   ```

7. Убедитесь, что ресурсы совместного использования для всех экземпляров IBM Spectrum Protect находятся на основном узле. Убедитесь, что у других узлов нет прав записи для этих ресурсов во время обновления. Если в среду входит несколько экземпляров сервера, то совместно используемые ресурсы для всех экземпляров должны быть доступными основному узлу.
8. На основном узле установите сервер V8.1.5, запустив команду ./install.sh. Инструкции смотрите в разделе Установка компонентов сервера. Запустив мастер, щелкните в окне IBM Installation Manager по значку Установить; не щелкайте по значкам Обновить и Изменить. Чтобы завершить обновление V6.3 до V8.1.5, необходимо установить сервер V8.1.5.
9. Запустите каждый сервер версии 8.1.5 в режиме активного окна:
   a. Убедитесь, что вы вошли в систему с ID владельца экземпляра.
   b. Перейдите в каталог экземпляра и введите следующую команду:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Подождите, пока вы не увидите сообщение сервера о том, что сервер запущен.

10. Остановите сервер для каждого обновляемого экземпляра IBM Spectrum Protect. Выполните команду:

    ```
    halt
    ```

11. На дополнительном узле кластера выполните следующие действия:
    a. Переместите все совместно используемые ресурсы на дополнительный узел. Если в среду входит несколько экземпляров сервера, то совместно используемые ресурсы для всех экземпляров должны в ходе обновления быть доступными дополнительным узлам.
    b. Остановите все экземпляры сервера. Убедитесь в отсутствии запущенных серверных процессов.
    c. Убедитесь, что менеджер баз данных не работает не на одном экземпляре. Определите, выполняются ли процессы db2sysc. Владелец выполняемых процессов указывает, какие экземпляры активны. Для каждого владельца экземпляра сервера введите следующую команду, чтобы остановить DB2:

       ```
       db2stop
       ```

    d. Установите сервер версии 8.1.5, запустив команду ./install.sh. Инструкции смотрите в разделе Установка компонентов сервера.
        i. Если вы используете мастер установки, то щелкните в окне IBM Installation Manager по значку Установить; не щелкайте по значкам Обновить и Изменить.
        ii. Если вы используете мастер установки, то выберите на странице Идентификационные данные экземпляра переключатель Конфигурировать этот экземпляр на дополнительном узле кластера для каждого конфигурируемого экземпляра.
        iii. Если вы устанавливаете сервер в режиме консоли, то в ответ на запрос `Конфигурировать этот экземпляр на дополнительном узле кластера?` введите `YES` (Да) для каждого экземпляра.
        iv. Если вы устанавливаете сервер в режиме без выдачи сообщений, то укажите `TRUE`в качестве значения переменной `user.`*`имя_экземпляра`*`_secondaryNode` для каждого экземпляра.
    e. Запустите все серверы версии 8.1.5. Если вы используете мониторинг на уровне приложений, то запустите сервер при помощи инструмента кластеризации.

       Инструкции по запуску сервера смотрите в разделе Запуск экземпляра сервера.

12. Зарегистрируйте лицензии для установленных в вашей системе компонентов сервера, введя команду REGISTER LICENSE:

    ```
    register license file=каталог_установки/server/bin/имя_компонента.lic
    ```

    Где *каталог_установки* указывает каталог, в который вы установили компонент, а *имя_компонента* указывает аббревиатуру для этого компонента.

    Например, если вы установили сервер в каталоге по умолчанию /opt/tivoli/tsm, введите следующую команду, чтобы зарегистрировать лицензию:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
    ```

    Например, если вы установили IBM Spectrum Protect Extended Edition в каталог /opt/tivoli/tsm, введите следующую команду:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
    ```

    Например, если вы установили IBM Spectrum Protect for Data Retention в каталог /opt/tivoli/tsm, введите следующую команду:

    ```
    register license file=/opt/tivoli/tsm/server/bin/dataret.lic
    ```

    Ограничение:
    Вы не можете использовать сервер IBM Spectrum Protect для регистрации лицензий на следующие продукты:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Команда REGISTER LICENSE не применяется к этим лицензиям. Лицензирование этих продуктов выполняется клиентами IBM Spectrum Protect.

Ссылки, связанные с данной:
BACKUP DB (Выполнить резервное копирование базы данных)
Команда BACKUP DEVCONFIG (создание резервных копий информации о конфигурации устройства)
BACKUP VOLHISTORY (сохранение информации хронологии томов с последовательным доступом)
HALT (выключение сервера)
REGISTER LICENSE (регистрация новой лицензии)
Операционные системы Linux

Обновление IBM Spectrum Protect до версии 8.1.5 в кластерной среде для Linux

Для использования новых функций IBM Spectrum Protect можно обновить сервер IBM Spectrum Protect, установленный в Linux в кластерной среде.

Процедура

Следуйте инструкциям в разделе Конфигурирование среды Linux для кластеризации.
Операционные системы Windows

Обновление сервера V6.3 или V7.1 до V8.1.5 в кластерной среде для Windows

Для использования новых функций продукта можно обновить сервер, установленный в операционной системе Windows в кластерной среде, с версии 6 или 7.1 до IBM Spectrum Protect версии 8.1.5.

Прежде чем начать

Убедитесь, что вы сохранили носитель установки базового выпуска сервера V6.3 или V7.1, который вы обновляете. Если вы устанавливали сервер из скачанного пакета, убедитесь, что доступны скачанные файлы. Если обновление завершится неудачно и модуль лицензий сервера будет деинсталлирован, вы должны будете переустановить лицензию с носителя установки базового выпуска сервера.

Процедура

1. Создайте резервную копию базы данных при помощи команды BACKUP DB. Рекомендуется использовать резервное копирование в режиме снимка, которое обеспечивает полное резервное копирование базы данных без прерывания запланированного резервного копирования. Например, можно ввести следующую команду, чтобы создать резервную копию снимка:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Создайте в другом каталоге резервную копию информации о конфигурации устройств. Выполните команду:

   ```
   backup devconfig filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация о конфигурации устройств.
3. Скопируйте файл хронологии томов в другой каталог. Выполните команду:

   ```
   backup volhistory filenames=имя_файла
   ```

   Где *имя_файла* - это имя файла, в котором будет храниться информация хронологии томов.
4. Сохраните копию файла серверных опций, называемого, как правило, dsmserv.opt и находящегося в каталоге экземпляра сервера.
5. Убедитесь, что группа ресурсов находится на основном узле и что все узлы в кластере запущены. Выполните на основном узле следующие действия:
   a. В окне Диспетчер отказоустойчивости кластеров переведите ресурс сервера в автономный режим и удалите его:
      i. Выберите Службы и приложения, а затем выберите группу кластеров. Ресурс сервера появится в разделе Другие ресурсы.
      ii. Выберите ресурс сервера и щелкните по Перевести этот ресурс в автономный режим.
      iii. Чтобы удалить ресурс сервера, выберите его и щелкните по Удалить.
   b. В окне Диспетчер отказоустойчивости кластеров удалите имя сети и IP-адрес:
      i. В разделе Имя сервера раскройте имя сети, чтобы посмотреть IP-адрес. Запишите имя сети и IP-адрес.
      ii. Выберите имя сети и IP-адрес и щелкните по Удалить.
   c. В окне Менеджер кластера переключения после отказа переведите ресурс сервера DB2 в автономный режим:
      i. Выберите Службы и приложения, а затем выберите группу кластеров. Ресурс сервера IBM Spectrum Protect появится в разделе Другие ресурсы.

ii. Выберите ресурс сервера DB2, например, SERVER1, и щелкните по Перевести этот ресурс в автономный режим.

6. Убедитесь, что сервер работает на первичном узле. Выполните на всех узлах кластера следующие шаги:
   a. Установите сервер IBM Spectrum Protect версии 8.1.5.
   b. Остановите службу кластеров. Единственный способ остановки службы кластеров - это использование приложения Службы. Щелкните правой кнопкой по Служба кластера и выберите Остановить.
   c. Удалите файлы tsmsvrrscexX64.dll и tsmsvrrscx64.dll из каталога C:\Windows\Cluster.
   d. Скопируйте следующие файлы DLL из каталога установки в каталог C:\Windows\Cluster:
      - tsmsvrrscexX64.dll
      - tsmsvrrscx64.dll
   e. Скопируйте следующий файл DLL из каталога установки в каталог C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
   f. Запустите службу кластеров. Единственный способ запустить службу кластеров - это использование приложения Службы. Щелкните правой кнопкой по Служба кластера и выберите Запустить.
7. В окне Менеджер отказоустойчивого кластера переместите экземпляр сервера IBM Spectrum Protect с первичного узла на другой узел в кластере.
8. Выполните на первичном узле следующие шаги:
   a. Установите сервер IBM Spectrum Protect версии 8.1.5.
   b. Остановите службу кластеров.
   c. Удалите файлы tsmsvrrscexX64.dll и tsmsvrrscx64.dll из каталога C:\Windows\Cluster.
   d. Скопируйте следующие файлы DLL из каталога установки в каталог C:\Windows\Cluster:
      - tsmsvrrscexX64.dll
      - tsmsvrrscx64.dll
   e. Скопируйте следующий файл DLL из каталога установки в каталог C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
   f. Запустите службу кластеров.
9. Необязательно: Переместите экземпляр сервера IBM Spectrum Protect обратно на первичный узел.

Дальнейшие действия

Если в Windows есть драйвер устройств для ленточных накопителей или чейнджеров носителей, которые вы собираетесь использовать, используйте этот драйвер устройств. Если драйвер устройства недоступен, то установите драйвер устройства IBM Spectrum Protect при помощи команды dpinst.exe /a. Файл dpinst.exe находится в каталоге драйверов устройств, положение которого по умолчанию - C:\Program Files\Tivoli\TSM\device\drivers.

Ссылки, связанные с данной:
BACKUP DB (Выполнить резервное копирование базы данных)
Команда BACKUP DEVCONFIG (создание резервных копий информации о конфигурации устройства)
BACKUP VOLHISTORY (сохранение информации хронологии томов с последовательным доступом)
REGISTER LICENSE (регистрация новой лицензии)
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Установка и обновление Центра операций

Центр операций IBM Spectrum Protect - это веб-интерфейс для управления средой хранения.

Прежде чем начать

Прежде чем приступить к установке и конфигурированию Центра операций, просмотрите следующую информацию:

- Требования к системе для Центра операций
  - Требования к компьютеру для Центра операций
  - Требования для хаб-сервера и подчиненных серверов
  - Требования к операционной системе
  - Требования к веб-браузеру
  - Требования языка
  - Требования и ограничения для службы управления клиентом
- ID администраторов, требуемые Центру операций
- IBM Installation Manager
- Контрольный список установки
- Получение установочного пакета Центра операций

Об этой задаче

В Табл. 1 перечислены методы установки и деинсталляции Центр операций и указано, где можно найти соответствующие инструкции.

Информацию об обновлении Центра операций смотрите в разделе Обновление компонента Центр операций.

Табл. 1. Методы установки и деинсталляции Центра операций.

Method	Инструкции
Мастер графики	• Установка Центра операций при помощи графического мастера • Деинсталляция Центра операций при помощи графического мастера
Режим консоли	• Установка Центра операций в режиме консоли • Деинсталляция Центра операций в режиме консоли
Режим без вывода сообщений	• Установка Центра операций в режиме без вывода сообщений • Деинсталляция Центра операций в режиме без вывода сообщений

- Планирование установки Центра операций
  Прежде чем приступать к установке Центра операций, нужно выяснить требования к системе, ID администраторов, которые требует Центр операций, и информацию, которую нужно предоставить программе установки.
- Установка Центра операций
  Центр операций можно установить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.
- Обновление компонента Центр операций
  Центр операций можно обновить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.
- Начинаем работу с Центром операций
  Перед тем, как вы сможете управлять средой хранения при помощи Центра операций, необходимо его сконфигурировать.
- Операционные системы AIXОперационные системы LinuxУстранение неполадок установки Центра операций
  Если в процессе установки Центра операций возникает проблема, которую вы не можете решить, вы можете поискать возможное решение в описаниях уже известных проблем.
- Деинсталляция Центра операций
  Центр операций можно деинсталлировать любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.
- Откат к предыдущей версии Центра операций
  По умолчанию IBM Installation Manager сохраняет предыдущие версии пакетов для выполнения отката, если с более поздними версиями обновлений, исправлений или пакетов возникает проблема.

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Планирование установки Центра операций

Прежде чем приступать к установке Центра операций, нужно выяснить требования к системе, ID администраторов, которые требует Центр операций, и информацию, которую нужно предоставить программе установки.

Об этой задаче

Из Центра операций можно управлять следующими основными аспектами среды хранения:

- Серверы и клиенты IBM Spectrum Protect
- Службы, такие, как служба резервного копирования и восстановления, архивирования и получения данных, а также перенастройки и возврата данных
- Пулы хранения и устройства хранения

Центр операций содержит следующие компоненты:

Пользовательский интерфейс для нескольких серверов
: С помощью Центра операций можно управлять одним или несколькими серверами IBM Spectrum Protect.

В среде с несколькими серверами можно задать один сервер в качестве *хаб-сервера*, а остальные - в качестве *подчиненных серверов*. Хаб-сервер может получать оповещения и информацию о состоянии от подчиненных серверов и выдавать эту информацию в консолидированном представлении в Центре операций.

Мониторинг оповещений

Оповещение - это уведомление о проблеме на сервере; оповещение инициализируется сообщением сервера. Вы можете указать, какие сообщения сервера инициализируют оповещения, и в Центре операций или в электронной почте только эти сообщения будут показаны как оповещения.

Мониторинг оповещений может помочь выявить и отследить ошибки на сервере.

Удобный интерфейс командной строки
Центр операций содержит интерфейс командной строки для поддержки расширенных функций и конфигурирования.

- Требования к системе для Центра операций
  Прежде чем устанавливать Центр операций, убедитесь, что ваша система соответствует минимальным требованиям.
- ID администраторов, требуемые Центру операций
  У администратора должны быть допустимые ID и пароль на хаб-сервере для входа в Центр операций. Кроме того, Центру операций назначается ID администратора, чтобы Центр операций мог отслеживать серверы.
- IBM Installation Manager
  Центр операций использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.
- Контрольный список установки
  Прежде чем приступить к установке компонента Центр операций, необходимо проверить определенную информацию, такую как идентификационные данные установки, и определить входные данные, которые нужно предоставить IBM Installation Manager для установки.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Требования к системе для Центра операций

Прежде чем устанавливать Центр операций, убедитесь, что ваша система соответствует минимальным требованиям.

Воспользуйтесь страницей Калькулятор требований к системе для Центра операций, чтобы оценить требования к системе для работы Центра операций, а также хаб-сервера и подчиненных серверов, которые отслеживает Центр операций.

Требования, проверяемые во время установки

В таблице Табл. 1 перечислены предварительные требования, проверяемые при установке, и указано, где найти дополнительную информацию об этих требованиях.

Табл. 1. Требования, проверяемые во время установки

Требование	**Подробности**
Минимальные требования к памяти	Требования к компьютеру для Центра операций
Требования операционной системы	Требования к операционной системе
Имя хоста для компьютера, где будет установлен Центр операций	Контрольный список установки
Требования для каталога установки Центр операций	Контрольный список установки

- Требования к компьютеру для Центра операций
  Центр операций можно установить на компьютер, на котором работает сервер IBM Spectrum Protect, или на другой компьютер. Если вы устанавливаете Центр операций на тот же компьютер, что и сервер, этот компьютер должен соответствовать требованиям к системе и для Центра операций, и для сервера.
- Требования для хаб-сервера и подчиненных серверов
  Когда вы впервые открываете Центр операций, вы должны связать Центр операций с одним сервером IBM Spectrum Protect, заданным в качестве *хаб-сервера*. В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

- Требования к операционной системе
  Центр операций доступен в системах AIX, Linux и Windows.
- Требования к веб-браузеру
  Центр операций работает в браузерах Apple, Google, Microsoft и Mozilla.
- Требования языка
  По умолчанию Центр операций использует язык, заданный для веб-браузера. Однако процесс установки использует язык операционной системы. Убедитесь, что для веб-браузера и операционной системы задан нужный язык.
- Требования и ограничения для службы управления клиентом
  Службы управления клиентом IBM Spectrum Protect - это компонент, устанавливаемый на клиентах резервного копирования и архивирования для сбора диагностической информации (например, файлов журнала клиента). Перед установкой компонента служба управления клиентами в вашей системе нужно ознакомиться с требованиями и ограничениями.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Требования к компьютеру для Центра операций

Центр операций можно установить на компьютер, на котором работает сервер IBM Spectrum Protect, или на другой компьютер. Если вы устанавливаете Центр операций на тот же компьютер, что и сервер, этот компьютер должен соответствовать требованиям к системе и для Центра операций, и для сервера.

Требования к ресурсам

Для запуска Центра операций требуются следующие ресурсы:

- Одно процессорное ядро
- 4 ГБ памяти
- 1 ГБ пространства на диске

Хаб-серверу и подчиненным серверам, которые отслеживает Центр операций, нужны дополнительные ресурсы, как описано в разделе Требования для хаб-сервера и подчиненных серверов.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Требования для хаб-сервера и подчиненных серверов

Когда вы впервые открываете Центр операций, вы должны связать Центр операций с одним сервером IBM Spectrum Protect, заданным в качестве *хаб-сервера*. В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

Подчиненные серверы отправляют оповещения и информацию о состоянии хаб-серверу. Центр операций содержит консолидированное представление оповещений и информации о состоянии для хаб-сервера и всех подчиненных серверов.

Если Центром операций отслеживается только один сервер, то этот сервер все равно называется хаб-сервером, хотя к нему не подключен ни один подчиненный сервер.

В таблице Табл. 1 указана версия сервера IBM Spectrum Protect, которая должна быть установлена на хаб-сервере и на каждом подчиненном сервере, которыми управляет Центр операций.

Табл. 1. Требования к версии сервера IBM Spectrum Protect для хаб-сервера и подчиненных серверов

Центр операций	Версия хаб-сервера	Версия на каждом подчиненном сервере
V8.1.5	V8.1.5	Версия 6.3.4 или новее Ограничение: Некоторые функции компонента Центр операций недоступны для серверов, использующих более раннюю версию, чем V8.1.5.

Число подчиненных серверов, которое может поддерживать хаб-сервер

Число подчиненных серверов, которое может поддерживать хаб-сервер, зависит от конфигурации и от версии IBM Spectrum Protect на каждом подчиненном сервере. Однако можно принять как общее правило то, что один хаб-сервер может поддерживать 10 - 20 подчиненных серверов V6.3.4, но большее количество подчиненных серверов V7.1 или новее.

- Советы по проектированию конфигурации хаб-сервера и подчиненных серверов
  При проектировании конфигурации хаб-сервера и подчиненных серверов следует внимательно отнестись к требованиям ресурсов для мониторинга состояния. Кроме того, решите, как вы хотите группировать хаб-сервер и подчиненные серверы и хотите ли вы использовать несколько хаб-серверов.
- Советы по выбору хаб-сервера
  Для хаб-сервера нужно выбрать сервер с достаточными ресурсами, расположенный так, чтобы обеспечить минимальную задержку двусторонней сетевой связи.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Советы по проектированию конфигурации хаб-сервера и подчиненных серверов

При проектировании конфигурации хаб-сервера и подчиненных серверов следует внимательно отнестись к требованиям ресурсов для мониторинга состояния. Кроме того, решите, как вы хотите группировать хаб-сервер и подчиненные серверы и хотите ли вы использовать несколько хаб-серверов.

Воспользуйтесь страницей Калькулятор требований к системе для Центра операций, чтобы оценить требования к системе для работы Центра операций, а также хаб-сервера и подчиненных серверов, которые отслеживает Центр операций.

Основные факторы, влияющие на производительность

На производительность Центра операций сильнее всего влияют следующие факторы:

- Процессор и память на компьютере, на котором установлен Центр операций
- Системные хаб-сервера и подчиненных серверов, включая дисковую систему, используемую для базы данных хаб-сервера.
- Число клиентских узлов и файловых пространств виртуальных машин, которые управляются хаб-сервером и подчиненными серверами
- Частота обновления данных в Центре операций

Как группировать хаб-сервер и подчиненные серверы

Группируйте хаб-сервер и подчиненные серверы по географическому положению. Например, управление серверами в пределах одного центра данных может предотвратить проблемы, связанные с брандмауэрами или недостаточной полосой пропускания между разными положениями. При необходимости серверы можно дополнительно подразделить в соответствии с одной или несколькими следующими характеристиками:

- Администратор, который управляет серверами.
- Объект организации, который финансирует серверы.
- Операционная система сервера
- Язык, на котором работают серверы
  Совет: Если хаб-сервер и подчиненные серверы работают на разных языках, то в Центре операций может выводится испорченный текст.

Как сгруппировать хаб-сервер и подчиненные серверы в конфигурации организации

В конфигурации организации сеть серверов IBM Spectrum Protect управляется как группа. Изменения, внесенные в *менеджере конфигурации*, можно автоматически распространить на один или несколько *управляемых серверов* в сети.

Обычно Центр операций регистрирует выделенный ID администратора на хаб-сервере и подчиненных серверах и управляет им. У этого *администратора мониторинга* всегда должен быть один и тот же пароль на всех серверах.

Если вы используете конфигурацию организации, то можно улучшить процесс синхронизации идентификационных данных администратора на подчиненных серверах. Чтобы повысить производительность и эффективность управления ID администратора, сделайте следующее:

1. Назначьте сервер менеджера конфигурации хаб-сервером Центра операций. Во время конфигурирования хаб-сервера регистрируется ID администратора мониторинга с именем IBM-OC-*имя_хаб-сервера*.
2. Добавьте на хаб-сервере ID администратора мониторинга в новый или в существующий профиль конфигурации организации. Введите команду NOTIFY SUBSCRIBERS, чтобы распространить профиль на управляемые серверы.
3. Добавьте один или несколько управляемых серверов в качестве подчиненных серверов Центра операций.

Центр операций обнаруживает эту конфигурацию и позволяет менеджеру конфигурации распространять ID администратора мониторинга на подчиненные серверы и изменять его.

Когда использовать несколько хаб-серверов

Если вы работаете больше, чем с 10-20 подчиненными серверами V6.3.4, или если из-за ограничений ресурсов требуется многораздельная среда, то вы можете сконфигурировать несколько хаб-серверов и подключить к каждому хаб-серверу поднабор подчиненных серверов.
Ограничения:

- Один сервер не может быть и хаб-сервером, и подчиненным сервером.
- Каждый подчиненный сервер может быть назначен только одному хаб-серверу.
- Для каждого хаб-сервера требуется отдельный экземпляр Центра операций, каждый из которых имеет свой веб-адрес.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Советы по выбору хаб-сервера

Для хаб-сервера нужно выбрать сервер с достаточными ресурсами, расположенный так, чтобы обеспечить минимальную задержку двусторонней сетевой связи.

Внимание: Не используйте один и тот же сервер в качестве хаб-сервера для нескольких Центров операций.
При выборе, какой сервер назначить хаб-сервером, руководствуйтесь следующими рекомендациями:

Выберите слабо нагруженный сервер
: Выберите сервер с небольшой нагрузкой для операций (например, для резервного копирования клиентов и архивирования). Слабо нагруженный сервер также хорошо использовать в качестве системы хоста для Центра операций.

  Убедитесь, что у сервера достаточно ресурсов для обслуживания и своей обычной рабочей нагрузки сервера, и оценочной нагрузки при работе в качестве хаб-сервера.

Расположите сервер так, чтобы обеспечить минимальную задержку двусторонней сетевой связи
: Расположите хаб-сервер так, чтобы сетевое соединение между хаб-сервером и подчиненными серверами имело двустороннюю задержку не более 5 мс. Эта задержка обычно может быть достигнута, когда серверы находятся в одной и той же локальной сети (LAN).

  Сети, которые плохо настроены, интенсивно используются другими приложениями или показывают двустороннюю задержку значительно больше 5 мс, могут ухудшить связь между хаб-сервером и подчиненными серверами. Например, двусторонняя задержка в 50 мс или выше может вызвать истечение срока ожидания связи, из-за чего подчиненные серверы будут отсоединяться от Центра операций или повторно соединяться с ним. Такие высокие задержки могут наблюдаться при связи через глобальные сети (wide area network, WAN) на большом расстоянии.

  Если подчиненные серверы находятся на большом расстоянии от хаб-сервера, и в Центре операций наблюдаются частые разрывы соединений, можно увеличить значение опции ADMINCOMMTIMEOUT на каждом сервере, чтобы уменьшить частоту возникновения этой проблемы.

Убедитесь, что хаб-сервер соответствует требованиям к ресурсам для мониторинга состояния
: Для мониторинга состояния требуются дополнительные ресурсы на каждом сервере, где он включен. Требуемые ресурсы зависят в первую очередь от числа клиентов, которые управляются хаб-сервером и подчиненными серверами. На хаб-сервере с подчиненным сервером V7.1 или новее используется меньше ресурсов, чем на хаб-сервере с подчиненным сервером V6.3.4.

  Убедитесь, что хаб-сервер соответствует требованиям к ресурсам использования процессора, пространства для базы данных, пространства для архивных журналов и мощности операций ввода-вывода в секунду (I/O operations per second, IOPS).

Хаб-сервер с высокой мощностью IOPS может обрабатывать больший объем данных о состоянии, приходящих с подчиненных серверов. Эту мощность можно обеспечить при использовании следующих устройств хранения для базы данных хаб-сервера:

- Твердотельный накопитель (SSD) уровня предприятия
- Внешнее устройство дискового хранения SAN с несколькими томами или несколькими дисководами в каждом томе.

В среде, содержащей менее 1000 клиентов, задайте для базы данных хаб-сервера базовую емкость 1000 IOPS, если хаб-сервер управляет подчиненными серверами.

Определите, нужно ли в вашей среде несколько хаб-серверов
Если одним набором хаб-сервера и подчиненных серверов управляется более 10 000 - 20 000 клиентских узлов и файловых пространств виртуальных машин, требования к ресурсам могут превышать доступные ресурсы хаб-сервера, особенно если подчиненные серверы - это серверы V6.3.4. Возможно, следует назначить хаб-сервером второй сервер и переместить часть подчиненных серверов на новый хаб-сервер для балансировки нагрузки.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Требования к операционной системе

Центр операций доступен в системах AIX, Linux и Windows.

Центр операций может работать в следующих системах:

- Операционные системы AIXСистемы AIX:
  - IBM® AIX V7.1 (64-разрядная версия) TL 4 и SP 2
  - IBM AIX V7.2 (64-разрядная версия) TL 0 и SP 2
- Операционные системы LinuxLinux в системах x86_64:
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 11 с Service Pack 4 или новее
  - SUSE Linux Enterprise Server 12
- Операционные системы LinuxСистемы Linux on System z (s390x, 64-разрядная архитектура):
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 12
- Операционные системы LinuxСистемы Linux on Power Systems (с прямым порядком байтов)
  - Red Hat Enterprise Linux 7.3 с архитектурой PPC64LE
- Операционные системы WindowsСистемы Windows:
  - Microsoft Windows Server 2012: Standard, Enterprise или Datacenter Edition (64-разрядная версия)
  - Microsoft Windows Server 2012 R2 (64-разрядная версия)
  - Microsoft Windows Server 2016

Самую последнюю информацию о требованиях смотрите в документе Требования к аппаратному и программному обеспечению.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Требования к веб-браузеру

Центр операций работает в браузерах Apple, Google, Microsoft и Mozilla.

Для оптимального просмотра Центра операций в браузере задайте в системе разрешение экрана, как минимум, 1024 X 768 пикселей.

Для оптимальной производительности используйте браузер с хорошей производительностью JavaScript и включите кэширование браузера.

Центр операций работает в следующих браузерах:

- Apple Safari на iPad
  Ограничение: Если Apple Safari работает в iOS 8.x или iOS 9.x, вы не сможете использовать самоподписанный сертификат для защищенных взаимодействий с центром операций, не произведя дополнительного

конфигурирования сертификата. Используйте сертификат сертификатора (certificate authority, CA) или сконфигурируйте самоподписанный сертификат нужным образом. Инструкции смотрите в техническом примечании по адресу: http://www.ibm.com/support/docview.wss?uid=swg21963153.

- Google Chrome 54 или новее
- Microsoft Internet Explorer 11 или новее
- Mozilla Firefox ESR 45 или версии 48 либо новее

Связь между компонентом Центр операций и веб-браузером должна быть защищена с использованием протокола Transport Layer Security (TLS) 1.2. Веб-браузер должен поддерживать протокол TLS 1.2, и этот протокол должен быть включен. Если эти требования не выполняются, в веб-браузере появится ошибка SSL.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Требования языка

По умолчанию Центр операций использует язык, заданный для веб-браузера. Однако процесс установки использует язык операционной системы. Убедитесь, что для веб-браузера и операционной системы задан нужный язык.

 Операционные системы AIX

Табл. 1. Значения языков Центра операций, которые можно использовать в системах AIX

Язык	**Значение опции языка**
Китайский упрощенный	zh_CN
Китайский упрощенный (UTF-8)	ZH_CN
Китайский традиционный (Big5)	Zh_TW
Китайский традиционный (UTF-8)	ZH_TW
Китайский традиционный (euc_tw)	zh_TW
Английский	en_US
Английский (UTF-8)	EN_US
Французский	fr_FR
Французский (UTF-8)	FR_FR
Немецкий	de_DE
Немецкий (UTF-8)	DE_DE
Итальянский	it_IT
Итальянский (UTF-8)	IT_IT
Японский (EUC)	ja_JP
Японский (PC)	Ja_JP
Японский (UTF-8)	JA_JP
Корейский	ko_KR
Корейский (UTF-8)	KO_KR
Бразильский португальский	pt_BR
Бразильский португальский (UTF-8)	PT_BR
Русский	ru_RU
Русский (UTF-8)	RU_RU
Испанский	es_ES
Испанский (UTF-8)	ES_ES

 Операционные системы Linux

Табл. 2. Значения языков Центра операций, которые можно использовать в системах Linux

Язык	Значение опции языка
Китайский упрощенный	zh_CN
Китайский упрощенный (GBK)	zh_CN.gb18030
Китайский упрощенный (UTF-8)	zh_CN.utf8
Китайский традиционный (Big5)	Zh_TW
Китайский традиционный (euc_tw)	zh_TW
Китайский традиционный (UTF-8)	zh_TW.utf8
Английский, США	en_US
Английский (UTF-8)	en_US.utf8
Французский	fr_FR
Французский (UTF-8)	fr_FR.utf8
Немецкий	de_DE
Немецкий (UTF-8)	de_DE.utf8
Итальянский	it_IT
Итальянский (UTF-8)	it_IT.utf8
Японский (EUC)	ja_JP
Японский (UTF-8)	ja_JP.utf8
Корейский	ko_KR
Корейский (UTF-8)	ko_KR.utf8
Бразильский португальский	pt_BR
Бразильский португальский (UTF-8)	pt_BR.utf8
Русский	ru_RU
Русский (UTF-8)	ru_RU.utf8
Испанский	es_ES
Испанский (UTF-8)	es_ES.utf8

Операционные системы Windows

Табл. 3. Значения языков Центра операций, которые можно использовать в системах Windows

Язык	Значение опции языка
Китайский упрощенный	chs
Китайский традиционный	cht
Английский	ameng
Французский	fra
Немецкий	deu
Итальянский	ita
Japanese (Shift-JIS)	jpn
Корейский	kor
Бразильский португальский	ptb
Русский	rus
Испанский	esp

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Требования и ограничения для службы управления клиентом

Службы управления клиентом IBM Spectrum Protect - это компонент, устанавливаемый на клиентах резервного копирования и архивирования для сбора диагностической информации (например, файлов журнала клиента). Перед установкой компонента служба управления клиентами в вашей системе нужно ознакомиться с требованиями и ограничениями.

В документации к службе управления клиентом *компьютер клиента* - это компьютер, на котором установлен клиент резервного копирования и архивирования.

Диагностическую информацию можно собрать только с клиентов Linux и Windows, но администраторы могут просматривать диагностическую информацию по компоненту Центр операций в операционных системах AIX, Linux или Windows.

Требования для службы управления клиентом

Перед установкой службы управления клиентом убедитесь, что выполнены следующие требования:

- Для удаленного доступа к клиенту у администратора Центра операций должны быть системные полномочия или один из следующих уровней полномочий клиента:
  - Полномочия Политика
  - Полномочия владельца клиента
  - Полномочия доступа к клиентскому узлу
- Убедитесь, что компьютер клиента соответствует следующим требованиям:
  - Службу управления клиентом можно установить только на компьютерах клиента со следующими операционными системами Linux или Windows:
    - Linux x86 (64-разрядные), поддерживаемые для клиента резервного копирования и архивирования.
    - Windows (32- и 64-разрядные), поддерживаемые для клиента резервного копирования и архивирования.
  - Для передачи данных между компонентом служба управления клиентами и компонентом Центр операций должен быть установлен протокол Transport Layer Security (TLS) 1.2. Предоставляется базовая аутентификация, и данные и информация аутентификации шифруются через канал SSL. TLS 1.2 и необходимые сертификаты SSL автоматически устанавливаются при установке компонента служба управления клиентами.
- На компьютерах клиента Linux для установки службы управления клиентом требуются полномочия пользователя root.
- Для компьютеров клиентов с несколькими клиентскими узлами (например, компьютеры клиентов Linux) убедитесь, что имя каждого узла уникально на компьютере клиента.
  Совет: После установки службы управления клиентом ее не нужно устанавливать повторно, так как служба может обнаруживать несколько файлов опций клиента.

Ограничения службы управления клиентом

Служба управления клиентом предоставляет базовые службы для сбора диагностической информации в клиентах резервного копирования и архивирования. Ниже перечислены ограничения для службы управления клиентом:

- Вы можете установить компонент служба управления клиентами только в системах с клиентами резервного копирования и архивирования, включая клиентов резервного копирования и архивирования, установленных на узлах перемещения данных для IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
- Установить компонент служба управления клиентами на других компонентах клиентов или в других продуктах IBM Spectrum Protect, у которых нет клиентов резервного копирования и архивирования, вы не можете.
- Если клиенты резервного копирования и архивирования защищены брандмауэром, убедитесь, что компонент Центр операций может соединиться с клиентами резервного копирования и архивирования через брандмауэр, используя порт, сконфигурированный для компонента служба управления клиентами. Порт по умолчанию - 9028, но его можно изменить.
- Служба управления клиентом сканирует все файлы журнала клиента, чтобы найти записи, созданные в течение предыдущих 72 часов.
- На странице Диагностика в Центре операций содержится основная диагностическая информация для клиентов резервного копирования и архивирования. Однако вам может понадобиться доступ к компьютеру клиента и дополнительная диагностическая информация для устранения некоторых проблем резервного копирования.
- Если общий размер файлов журнала ошибок клиента и файлов журнала расписания больше 500 МБ, то при отправке записей журнала в Центр операций могут возникнуть задержки. Для управления размером файлов

журнала можно разрешить сокращение или перенос файлов журнала при помощи опций клиента errorlogretention или errorlogmax.
- Если вы используете одно и то же имя клиентского узла для соединения с несколькими серверами IBM Spectrum Protect, которые установлены на одном и том же сервере, вы можете посмотреть файлы журнала только для одного из клиентских узлов.

Информацию о служба управления клиентами, включая требования, ограничения и обновления документации, смотрите в техническом замечании 1963610.

Задачи, связанные с данной:
Сбор диагностической информации посредством службы управления клиентом Tivoli Storage Manager
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

ID администраторов, требуемые Центру операций

У администратора должны быть допустимые ID и пароль на хаб-сервере для входа в Центр операций. Кроме того, Центру операций назначается ID администратора, чтобы Центр операций мог отслеживать серверы.

Центр операций требует следующие ID администраторов IBM Spectrum Protect:

ID администраторов, зарегистрированные на хаб-сервере
Для входа в Центр операций можно использовать любой ID администратора, зарегистрированный на хаб-сервере. Уровень полномочий ID определяет, какие задачи можно выполнять. Создать ID администраторов можно командой REGISTER ADMIN.
Ограничение: Для использования ID администратора в конфигурации с несколькими серверами он должен быть зарегистрирован на хаб-сервере и подчиненных серверах с одинаковыми паролями и уровнями полномочий.
Для управления аутентификацией для этих серверов выберите один из следующих способов:

- Сервер LDAP (Lightweight Directory Access Protocol)
- Функции конфигурирования организации для автоматического распределения изменений определения администратора.

ID администратора мониторинга
При начальном конфигурировании хаб-сервера ID администратора IBM-ОС-*имя_сервера* регистрируется с системными полномочиями на хаб-сервере и связывается с начальным паролем, заданным вами. Этот ID, иногда называемый *администратор мониторинга*, предназначен для использования только Центром операций.

Не удаляйте, не блокируйте и не изменяйте этот ID. Тот же ID администратора с тем же паролем регистрируется на добавленных подчиненных серверах. Пароль автоматически изменяется на хаб-сервере и на подчиненных серверах каждые 90 дней. Вам не нужно использовать этот пароль или управлять им.

Ограничение: Центр операций управляет ID и паролем администратора мониторинга на подчиненных серверах, если только вы не используете для управления этими идентификационными данными конфигурацию организации. Дополнительную информацию об использовании конфигурации организации для управления идентификационными данными смотрите в разделе Советы по проектированию конфигурации хаб-сервера и подчиненных серверов.

Ссылки, связанные с данной:
REGISTER ADMIN (регистрация ID администратора)
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

IBM Installation Manager

Центр операций использует IBM® Installation Manager - программу установки, которая может использовать удаленные или локальные репозитории программ для установки или обновления многих продуктов IBM.

Если обязательная версия IBM Installation Manager еще не установлена, то она автоматически устанавливается или обновляется при установке Центра операций. Она должна остаться установленной на компьютере, чтобы позже можно было обновить или деинсталлировать Центр операций.

Ниже приведены объяснения некоторых терминов, используемых в IBM Installation Manager:

Предложение

Устанавливаемый модуль программного продукта.

Предложение Центра операций содержит все носители, которые требуются IBM Installation Manager для установки Центра операций.

Пакет
: Группа программных компонентов, необходимых для установки предложения.
Пакет Центр операций включает в себя следующие компоненты:

- Программу установки IBM Installation Manager
- Предложение Центр операций

Группа пакетов
: Набор пакетов, использующих общий родительский каталог.

Репозиторий
: Удаленная или локальная область хранения данных и других ресурсов приложения.

Пакет Центра операций хранится в репозитории в IBM Fix Central.

Каталог общих ресурсов
: Каталог, содержащий файлы или модули plugin программ, которые совместно используются пакетами.

IBM Installation Manager хранит в каталоге общих ресурсов связанные с установкой файлы, включая файлы, используемые для отката к предыдущей версии Центр операций.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Контрольный список установки

Прежде чем приступить к установке компонента Центр операций, необходимо проверить определенную информацию, такую как идентификационные данные установки, и определить входные данные, которые нужно предоставить IBM® Installation Manager для установки.

В следующем контрольном списке перечислена информация, которую надо проверить или определить, прежде чем приступать к установке Центр операций; в таблице Табл. 1 дано подробное описание этой информации:

- ☐ Проверьте имя хоста для компьютера, на котором устанавливается Центр операций.
- ☐ Проверьте идентификационные данные для установки.
- ☐ Определите каталог установки Центра операций, если не хотите принимать путь по умолчанию.
- ☐ Определите каталог установки IBM Installation Manager, если не хотите принимать путь по умолчанию.
- ☐ Определите порт, который должен использоваться веб-сервером Центра установки, если не хотите принимать номер порта по умолчанию.
- ☐ Определите пароль для защищенной связи.

Табл. 1. Информация, которую нужно проверить или определить, прежде чем приступать к установке Центра операций

Информация	**Подробности**
Имя хоста для компьютера, на котором нужно установить Центр операций.	Имя хоста должно отвечать следующим критериям: • Оно не должно содержать двухбайтные символы (DBCS) или символы подчеркивания (_). • Имя хоста может содержать символ дефиса (-), но это не должен быть последний символ в имени.
Идентификационные данные для установки	Для установки Центра операций следует использовать следующую учетную запись пользователя: •  Операционные системы AIX  Операционные системы LinuxПользователь root •  Операционные системы WindowsАдминистратор

Информация	Подробности

Каталог установки Центра операций	Центр операций устанавливается в подкаталог ui каталога установки.
	
	Следующие каталоги - это каталоги установки Центра операций по умолчанию:
	
	• Операционные системы AIX Операционные системы Linux/opt/tivoli/tsm
	Например, если вы используете каталог по умолчанию, то Центр операций устанавливается в следующий каталог:
	`/opt/tivoli/tsm/ui`
	• Операционные системы Windowsc:\Program Files\Tivoli\TSM
	Например, если вы используете каталог по умолчанию, то Центр операций устанавливается в следующий каталог:
	`c:\Program Files\Tivoli\TSM\ui`
	
	Имя каталога установки должно соответствовать следующим критериям:
	
	• Имя каталога может содержать не более 128 символов.
	• Имя каталога должно содержать только символы ASCII.
	• Имя каталога не должно содержать не показываемые символы управления.
	• Имя каталога не должно содержать следующие символы:
	`% | < > ' " $ & ; *`

Каталог установки IBM Installation Manager	Следующие каталоги - это каталоги установки IBM Installation Manager по умолчанию: • Операционные системы AIX Операционные системы Linux /opt/IBM/InstallationManager • Операционные системы WindowsC:\Program Files\IBM\Installation Manager
Номер порта, используемый веб-сервером компонента Центр операций.	Номер защищенного (https) порта должен соответствовать следующим критериям: • Этот номер должен быть целым числом в диапазоне 1024 - 65535. • Этот номер не должен уже использоваться или быть выделенным другим программам. Если номер порта не указан, то используется значение по умолчанию `11090`. Совет: Если позже вы забудете указанный вами номер порта, найдите его в следующем файле, где *каталог_установки* - это каталог, куда установлен Центр операций: • Операционные системы AIX Операционные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer/bootstrap.properties • Операционные системы Windows *каталог_установки*\ui\Liberty\usr\servers\guiServer\bootstrap.properties Файл bootstrap.properties содержит информацию для соединения с сервером IBM Spectrum Protect.

Информация	Подробности
Пароль для защищенной связи	Центр операций использует протокол HTTPS (Hypertext Transfer Protocol Secure) для связи с веб-браузерами. Для компонента Центр операций требуется защищенная связь между сервером и компонентом Центр операций. Для защиты связи нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл склада доверенных сертификатов компонента Центр операций. Файл склада доверенных сертификатов компонента Центр операций содержит сертификат, который Центр операций использует для связи HTTPS с веб-браузерами. При установке Центра операций вы создаете пароль для файла доверенного хранилища. При настройке защищенной связи между компонентом Центр операций и хаб-сервером нужно использовать тот же пароль для добавления сертификата хаб-сервера в файл склада доверенных сертификатов. Пароль для доверенного хранилища должен отвечать следующим критериям: • Пароль должен содержать не менее 6 и не более 64 символов. • Пароль должен содержать, как минимум, следующие символы: ○ Одну заглавную букву (A – Z) ○ Одну строчную букву (a – z) ○ Одну цифру (0 – 9) ○ Два символа, не являющихся алфавитно-цифровыми, которые указаны в следующем ряду: `~ @ # $ % ^ & * _ - + = ` |`  `( ) { } [ ] : ; < > , . ? /`

Задачи, связанные с данной:
Конфигурирование для защищенной связи
Переустановка пароля файла доверенного хранилища Центра операций
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Установка Центра операций

Центр операций можно установить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Прежде чем начать

Чтобы сконфигурировать Центр операций, нужно установить, сконфигурировать и запустить сервер IBM Spectrum Protect. Поэтому перед установкой Центра операций установите подходящий пакет сервера в соответствии с требованиями к версии сервера, приведенными в разделе Требования для хаб-сервера и подчиненных серверов.

Центр операций можно установить на компьютер, на котором установлен сервер IBM Spectrum Protect, или на другой компьютер.

- Получение установочного пакета Центра операций
  Пакет установки можно получить с сайта скачивания IBM®, например, IBM Passport Advantage или IBM Fix Central.
- Установка Центра операций при помощи графического мастера
  Центр операций можно установить или обновить при помощи графического мастера IBM Installation Manager.
- Установка Центра операций в режиме консоли
  Центр операций можно установить или обновить из командной строки в режиме консоли.
- Установка Центра операций в режиме без вывода сообщений
  Центр операций можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Получение установочного пакета Центра операций

Пакет установки можно получить с сайта скачивания IBM®, например, IBM Passport Advantage или IBM Fix Central.

Об этой задаче

После получения пакета с сайта загрузок IBM вы должны извлечь установочные файлы.

Процедура

Выполните описанные ниже шаги, чтобы извлечь файлы установки компонента Центр операций. В следующих шагах замените *номер_версии* на устанавливаемую вами версию компонента Центр операций.

 Операционные системы AIXВ системах AIX:

a. Скачайте следующий файл пакета в каталог по вашему выбору:

```
номер_версии.000
-IBM-SPOC-AIX.bin
```

b. Убедитесь, что у вас есть разрешения на выполнение для файла пакета.
Если нужно, то измените разрешения для файла, введя следующую команду:

```
chmod a+x номер_версии.000-IBM-SPOC-AIX.bin
```

c. Чтобы извлечь файлы установки, введите следующую команду:

```
./номер_версии.000-IBM-SPOC-AIX.bin
```

Самоизвлекающийся файл пакета извлекается в каталог.

 Операционные системы LinuxВ системах Linux:

a. Скачайте один из следующих файлов пакетов в каталог по вашему выбору:
   - *номер_версии*.000-IBM-SPOC-LinuxS390.bin
   - *номер_версии*.000-IBM-SPOC-Linuxx86_64.bin

b. Убедитесь, что у вас есть разрешения на выполнение для файла пакета.
Если нужно, то измените разрешения для файла, введя следующую команду:

```
chmod a+x имя_пакета.bin
```

c. Чтобы извлечь файлы установки, введите следующую команду:

```
./имя_пакета.bin
```

Самоизвлекающийся файл пакета извлекается в каталог.

 Операционные системы WindowsВ системах Windows:

a. Скачайте следующий файл пакета в каталог по вашему выбору:

```
номер_версии.000-IBM-SPOC-WindowsX64.exe
```

b. Дважды щелкните в проводнике Windows по имени файла, чтобы извлечь файлы установки.

Самоизвлекающийся файл пакета извлекается в каталог.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Установка Центра операций при помощи графического мастера

Центр операций можно установить или обновить при помощи графического мастера IBM® Installation Manager.

 Операционные системы AIX

Прежде чем начать

Если перечисленные ниже файлы RPM не установлены на компьютере, то установите их. Инструкции смотрите в разделе Установка файлов RPM для графического мастера.

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm
- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm
- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm

Процедура

1. Введите в каталоге, в который вы извлекли файл пакета установки Центра операций, следующую команду:
   - Операционные системы AIXОперационные системы Linux`./install.sh`
   - Операционные системы Windows`install.bat`
2. Выполните инструкции мастера, чтобы установить пакеты IBM Installation Manager и Центра установки.
   Операционные системы AIXЕсли ваша локаль использует кодировку UTF-8, то вы можете получить следующее сообщение и мастер установки будет работать медленно:

   ```
   Невозможно создать набор шрифтов
   ```

   Если появилось это сообщение, то выполните одно из следующих действий:
   - Задайте локаль, которая не использует UTF-8. Информацию о значениях опций языков, которые не используют UTF-8, смотрите в разделе Требования языка.
   - Установите Центр операций из командной строки в режиме консоли.
   - Установите Центр операций в режиме без вывода сообщений.

Дальнейшие действия

Смотрите раздел Конфигурирование центра операций.

- Операционные системы AIXУстановка файлов RPM для графического мастера
  Чтобы можно было использовать графический мастер IBM Installation Manager для установки Центра операций, нужно установить несколько файлов RPM.

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Установка Центра операций в режиме консоли

Центр операций можно установить или обновить из командной строки в режиме консоли.

Процедура

1. Запустите из каталога, в который вы извлекли файл пакета установки, следующую программу:
   Операционные системы AIXОперационные системы Linux

   ```
   ./install.sh -c
   ```

   Операционные системы Windows

   ```
   install.bat -c
   ```

2. Выполните инструкции в консоли, чтобы установить пакеты Installation Manager и Центра установки.

Дальнейшие действия

Смотрите раздел Конфигурирование центра операций.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Установка Центра операций в режиме без вывода сообщений

Центр операций можно установить или обновить в режиме без вывода сообщений. В режиме без вывода сообщений установка не отправляет сообщений на консоль, а сохраняет сообщения и ошибки в файлы журнала.

Прежде чем начать

Чтобы задать входные данные при использовании установки в режиме без вывода сообщений, можно использовать файл ответов. Указанные ниже примеры файлов ответов поставляются в каталоге input в том месте, куда был распакован пакет установки:

install_response_sample.xml
: Используйте этот файл для установки Центр операций.

update_response_sample.xml
: Используйте этот файл для обновления Центр операций.

Эти файлы содержат значения по умолчанию, которые помогут вам избежать всех ненужных предупреждений. Чтобы воспользоваться этими файлами, выполните приведенные в файлах инструкции.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. Создайте файл ответов. Вы можете изменить пример файла ответов или создать свой собственный.
   Совет: Чтобы сгенерировать файл ответов в ходе установки в режиме консоли, выберите опции установки в режиме консоли. Затем введите на панели Сводка `G`, чтобы сгенерировать файл ответов в соответствии с опциями, выбранными ранее.
2. Создайте пароль для склада доверенных сертификатов компонента Центр операций в файле ответов.
   Если вы используете файл install_response_sample.xml, добавьте пароль в следующую строку в файле, где *`пароль`* - это пароль:

   ```
   <variable
   name='ssl.password' value='пароль' />
   ```

   Дополнительную информацию об этом пароле смотрите в разделе Контрольный список установки.
   Совет: Пароль склада доверенных сертификатов не требуется, если вы используете файл update_response_sample.xml для обновления компонента Центр операций.
3. Запустите установку без вывода сообщений, введя в каталоге, в который распакован пакет установки, следующую команду. Значение *файл_ответов* соответствует пути и имени файла ответов:
   - Операционные системы AIX Операционные системы Linux

     ```
     ./install.sh -s -input файл_ответов
     -acceptLicense
     ```

   - Операционные системы Windows

     ```
     install.bat -s -input файл_ответов -acceptLicense
     ```

Дальнейшие действия

Смотрите раздел Конфигурирование центра операций.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Обновление компонента Центр операций

Центр операций можно обновить любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

Прежде чем начать

Перед обновлением Центра операций ознакомьтесь с требованиями к системе и с контрольным списком установки. У новой версии Центра операций могут быть дополнительные или другие требования по сравнению с версией, которую вы используете в настоящий момент.

Об этой задаче

Инструкции по обновлению Центра операций совпадают с инструкциями по установке Центра операций за следующими исключениями:

- Используйте функцию Обновить программы IBM® Installation Manager, а не функцию Установить.
  Совет: В IBM Installation Manager термин *обновить* (update) означает поиск и установку обновлений и исправлений для установленных программных пакетов. В этом контексте термины *update* и *upgrade* - это синонимы.
- Если вы обновляете Центр операций в режиме без вывода сообщений, то вы можете пропустить шаг создания пароля для файла доверенного хранилища.

Операционные системы AIX Операционные системы Linux Операционные системы Windows

Начинаем работу с Центром операций

Перед тем, как вы сможете управлять средой хранения при помощи Центра операций, необходимо его сконфигурировать.

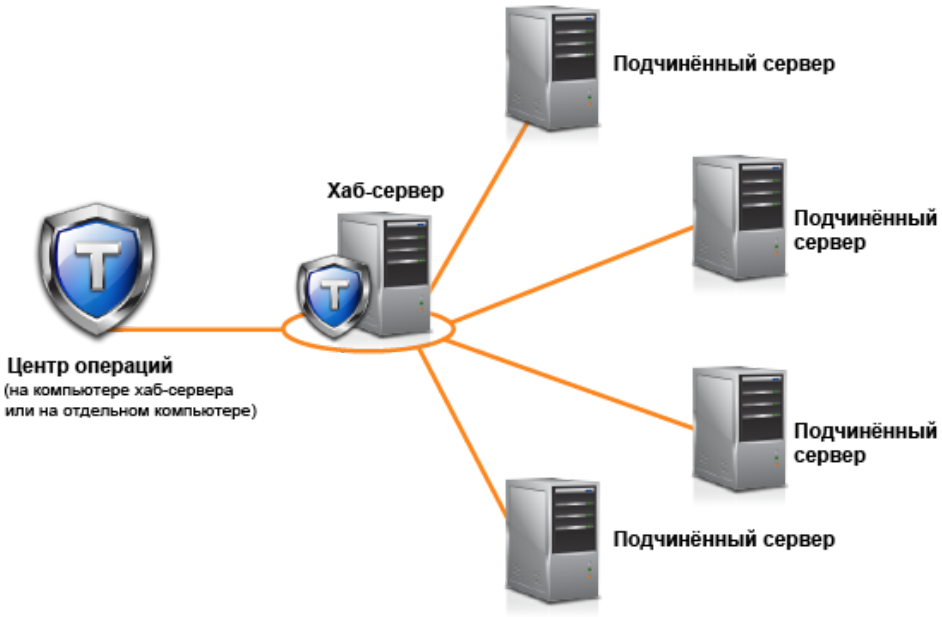
Об этой задаче

После установки Центра операций выполните следующие базовые действия конфигурирования:

1. Определите хаб-сервер.
2. Добавьте подчиненные серверы.
3. При необходимости сконфигурируйте оповещения по электронной почте на хаб-сервере и подчиненных серверах.

Рис. 1 иллюстрирует конфигурацию Центра операций.

Рис. 1. Пример конфигурации Центра операций с хаб-сервером и подчиненными серверами



- Конфигурирование центра операций
  Если вы открываете Центр операций впервые, то его нужно сконфигурировать для управления средой хранения. Вы должны связать Центр операций с сервером IBM Spectrum Protect, заданным в качестве хаб-сервера. После этого можно подключить дополнительные серверы IBM Spectrum Protect как подчиненные серверы.
- Конфигурирование для защищенной связи
  Центр операций использует протокол HTTPS (Hypertext Transfer Protocol Secure) для связи с Web-браузерами.

Протокол Transport Layer Security (TLS) защищает связь между Центром операций и хаб-сервером, а также между хаб-сервером и связанными подчиненными серверами.

- Запуск и остановка веб-сервера
  Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.
- Открытие Центра операций
  Страница Обзор - это начальное представление по умолчанию в Центре операций. Однако в веб-браузере можно поместить в закладки страницу, которую вы хотите открывать при входе в Центр операций.
- Сбор диагностической информации посредством службы управления клиентом Tivoli Storage Manager
  служба управления клиентами собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает ее доступной для Центра операций для основных функций мониторинга.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Конфигурирование центра операций

Если вы открываете Центр операций впервые, то его нужно сконфигурировать для управления средой хранения. Вы должны связать Центр операций с сервером IBM Spectrum Protect, заданным в качестве хаб-сервера. После этого можно подключить дополнительные серверы IBM Spectrum Protect как подчиненные серверы.

- Назначение хаб-сервера
  Когда вы в первый раз соединяетесь с Центром операций, вы должны указать, какой сервер IBM Spectrum Protect является хаб-сервером.
- Добавление подчиненного сервера
  После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.
- Отправка оповещений администраторам по электронной почте
  Оповещение - это уведомление о проблеме на сервере IBM Spectrum Protect; оповещение инициализируется сообщением сервера. Оповещения могут быть показаны в Центр операций; сервер может отправлять оповещения администраторам по электронной почте.
- Добавление настроенного текста в окно входа в систему
  Вы можете добавить пользовательский текст (например, Условия использования программы вашей организации) в окно входа в Центр операций, чтобы пользователи Центра операций видели этот текст перед вводом имени пользователя и пароля.
- Как включить службы REST
  Приложения, которые используют службы Representational State Transfer (REST), могут запрашивать среду хранения и управлять средой хранения, соединяясь с центром операций.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Назначение хаб-сервера

Когда вы в первый раз соединяетесь с Центром операций, вы должны указать, какой сервер IBM Spectrum Protect является хаб-сервером.

Прежде чем начать

Для компонента Центр операций требуется защищенная связь между хаб-сервером и компонентом Центр операций. Для защиты связи нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл склада доверенных сертификатов компонента Центр операций. Дополнительные сведения смотрите в разделе Защита связи между Центром операций и хаб-сервером.

Процедура

В браузере введите следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

```
https://имя_хоста:защищенный_порт/oc
```

Советы:

- В URL учитывается регистр символов. Например, убедитесь, что вы ввели "oc" строчными буквами, как это показано.
- Дополнительную информацию о номере порта смотрите в разделе Контрольный список установки.
- Если вы подключаетесь к Центру операций впервые, то вы должны предоставить следующую информацию:
  - Информация о соединении для сервера, который вы хотите назначить хаб-сервером
  - Идентификационные данные входа в систему для администратора, который задан для этого сервера
- Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как хаб-сервер.

Дальнейшие действия

Если в среде есть несколько серверов IBM Spectrum Protect, то добавьте на хаб-сервер остальные серверы как подчиненные серверы.

Внимание: Не изменяйте имя сервера после того, как он сконфигурирован в качестве хаб-сервера или подчиненного сервера.

Понятия, связанные с данным:
Требования для хаб-сервера и подчиненных серверов
ID администраторов, требуемые Центру операций
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Добавление подчиненного сервера

После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.

Прежде чем начать

Связь между подчиненным сервером и хаб-сервером должна быть защищена с использованием протокола Transport Layer Security (TLS). Для защиты связи добавьте сертификат подчиненного сервера в файл доверенных сертификатов хаб-сервера.

Процедура

1. Щелкните в панели меню Центр операций по Серверы. Откроется страница Серверы.

   В таблице на странице Серверы состоянием сервера может быть "Не отслеживается" Это состояние означает, что хотя администратор и определил этот сервер на хаб-сервере при помощи команды DEFINE SERVER, этот сервер еще не сконфигурирован в качестве подчиненного сервера.

2. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по Отслеживать подчиненный.
   - Если сервера, который вы хотите добавить, нет в таблице, а защищенная связь SSL/TLS не требуется, то щелкните по + Подчиненный в панели меню таблицы.
3. Задайте нужную информацию и выполните действия в мастере конфигурирования подчиненных серверов.
   Совет: Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как подчиненный сервер.

Ссылки, связанные с данной:
DEFINE SERVER (Задать сервер для обмена данными между серверами)
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Отправка оповещений администраторам по электронной почте

Оповещение - это уведомление о проблеме на сервере IBM Spectrum Protect; оповещение инициализируется сообщением сервера. Оповещения могут быть показаны в Центр операций; сервер может отправлять оповещения администраторам по электронной почте.

Прежде чем начать

Прежде чем конфигурировать уведомления по электронной почте об оповещениях для администраторов, убедитесь, что выполнены следующие требования:

- Для отправки и получения оповещений по электронной почте требуется сервер SMTP; у сервера, который отправляет оповещения по электронной почте, должен быть доступ к серверу SMTP.
  Совет: Если Центр операций установлен на отдельном компьютере, этому компьютеру не нужен доступ к серверу SMTP.
- У администратора должна быть системная привилегия для конфигурирования отправки уведомлений по электронной почте.

Об этой задаче

Уведомление по электронной почте отправляется только для первого возникновения оповещения. Кроме того, если оповещение сгенерировано до того, как вы сконфигурировали уведомление по электронной почте, для этого оповещения не отправляется уведомление по электронной почте.

Уведомления по электронной почте можно сконфигурировать следующими способами:

- Отправка уведомлений для отдельных оповещений
- Отправка сводки оповещений

Сводка оповещений содержит информацию о текущих оповещениях. В сводке указаны общее число оповещений, общее число активных и неактивных оповещений, самое старое оповещение, самое новое оповещение и наиболее часто встречающееся оповещение.

Можно указать до трех администраторов, получающих сводки оповещений по электронной почте. Сводки оповещений отправляются примерно раз в час.

Процедура

Чтобы сконфигурировать уведомления по электронной почте об оповещениях для администраторов, выполните следующие действия на каждом хаб-сервере и подчиненном сервере, от которых вы хотите получать оповещения по электронной почте.

1. Чтобы проверить, включен ли мониторинг оповещений, введите следующую команду:

   ```
   QUERY MONITORSETTINGS
   ```

2. Если в выводе этой команды говорится, что мониторинг оповещений выключен, введите следующую команду. В ином случае переходите к следующему шагу.

   ```
   SET ALERTMONITOR ON
   ```

3. Чтобы включить отправку уведомлений по электронной почте, введите следующую команду:

   ```
   SET ALERTEMAIL ON
   ```

4. Чтобы определить сервер SMTP, используемый для отправки уведомлений по электронной почте, введите следующую команду:

   ```
   SET ALERTEMAILSMTPHOST имя_хоста
   ```

5. Чтобы указать номер порта для сервера SMTP, введите следующую команду:

   ```
   SET ALERTEMAILSMTPPORT номер_порта
   ```

   Номер порта по умолчанию - 25.

6. Чтобы указать адрес электронной почты отправителя оповещений, введите следующую команду:

   ```
   SET ALERTEMAILFROMADDR адрес_электронной_почты
   ```

7. Для каждого ID администратора, который должен получать уведомления по электронной почте, введите одну из следующих команд, чтобы активировать уведомления по электронной почте и задать адрес электронной почты:

   ```
   REGISTER ADMIN имя_администратора ALERT=YES EMAILADDRESS=адрес_электронной_почты
   ```

   ```
   UPDATE ADMIN имя_администратора ALERT=YES EMAILADDRESS=адрес_электронной_почты
   ```

8. Выберите любую из следующих опций (или обе этих опции) и укажите ID администраторов, которые должны получать уведомления по электронной почте:
   - Отправка уведомлений для отдельных оповещений
     Для указания или изменения ID администраторов, которые должны получать уведомления по электронной почте для отдельного оповещения, введите одну из следующих команд:

     ```
     DEFINE ALERTTRIGGER номер_сообщения ADmin=имя_администратора_1,имя_администратора_2
     ```

     ```
     UPDATE
     ALERTTRIGGER номер_сообщения ADDadmin=имя_администратора_3
     DELadmin=имя_администратора_1
     ```

     Совет: На странице Сконфигурировать оповещения Центра операций можно выбрать администраторов, которые будут получать уведомления по электронной почте.
   - Отправка сводки оповещений
     Чтобы задать или изменить ID администраторов для получения сводки оповещений по электронной почте, введите следующую команду:

     ```
     SET ALERTSUMMARYTOADMINS имя_администратора1,имя_администратора2,имя_администратора3
     ```

   Если вы хотите получать сводки оповещений, но не хотите получать уведомления об отдельных оповещениях, то сделайте следующее:
   a. Приостановите уведомления об отдельных оповещениях, как описано в разделе Временная приостановка отправки оповещений по электронной почте.
   b. Убедитесь, что соответствующий ID администратора указан в следующей команде:

      ```
      SET ALERTSUMMARYTOADMINS имя_администратора1,имя_администратора2,имя_администратора3
      ```

Отправка оповещений нескольким администраторам по электронной почте

В следующем примере показаны команды, которые инициируют отправку по электронной почте всех оповещений для сообщения ANR1075E администраторам `myadmin`, `djadmin` и `csadmin`:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

- Временная приостановка отправки оповещений по электронной почте
  Бывают ситуации, когда нужно временно приостановить оповещения по электронной почте. Например, вы хотите получать сводни оповещений, но приостановить уведомления об отдельных оповещениях, или вы хотите приостановить отправку оповещений по электронной почте, если администратор находится в отпуске.

Ссылки, связанные с данной:
DEFINE ALERTTRIGGER (задать триггер оповещения)
QUERY MONITORSETTINGS (Запрос параметров конфигурации для оповещений мониторинга и состояния сервера)
REGISTER ADMIN (регистрация ID администратора)
SET ALERTEMAIL (Задание монитора оповещений для оповещения администраторов по электронной почте)
SET ALERTEMAILFROMADDR (Задать адрес электронной почты отправителя)
SET ALERTEMAILSMTPHOST (Задать имя хоста почтового сервера SMTP)
SET ALERTEMAILSMTPPORT (Задать порт хоста почтового сервера SMTP)
SET ALERTMONITOR (Включить или выключить мониторинг оповещений)
SET ALERTSUMMARYTOADMINS (Задать список администраторов, получающих по электронной почте сводку оповещений)
UPDATE ADMIN (обновление администратора)
UPDATE ALERTTRIGGER (Изменить триггер оповещения)
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Добавление настроенного текста в окно входа в систему

Вы можете добавить пользовательский текст (например, Условия использования программы вашей организации) в окно входа в Центр операций, чтобы пользователи Центра операций видели этот текст перед вводом имени пользователя и

пароля.

Процедура

Чтобы добавить пользовательский текст в экран входа в систему, сделайте следующее:

1. На компьютере с установленным продуктом Центр операций перейдите в следующий каталог, где *каталог_установки* представляет собой каталог, в котором установлен продукт Центр операций:

    Операционные системы AIX  Операционные системы Linux*каталог_установки*/ui/Liberty/usr/servers/guiServer

    Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer

2. Создайте в каталоге файл loginText.html, содержащий текст, который вы хотите добавить в экран входа в систему. Текст, содержащий специальные символы и символы не ASCII, должен быть в кодировке UTF-8.
   Совет: Можно сформатировать текст, добавив теги HTML.
3. Проверьте добавленный текст в окне входа в Центр операций.
   Чтобы открыть Центр операций, введите в веб-браузере следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

   `https://`*`имя_хоста`*`:`*`защищенный_порт`*`/oc`

Как включить службы REST

Приложения, которые используют службы Representational State Transfer (REST), могут запрашивать среду хранения и управлять средой хранения, соединяясь с центром операций.

Об этой задаче

Включите эту функцию, чтобы разрешить службам REST взаимодействовать с хаб-серверами и подчиненными серверами путем отправки вызовов по следующему адресу:

`https://`*`имя_хоста_цо`*`:`*`порт`*`/oc/api`

где *имя_хоста_цо* - это сетевое имя или IP-адрес хост-системы центра операций, а *порт* - это номер порта центра операций. Номер порта по умолчанию - 11090.
Чтобы получить информацию о службах REST, доступных для центра операций, смотрите техническое примечание http://www-01.ibm.com/support/docview.wss?uid=swg21997347 или введите следующий вызов REST:

`https://`*`имя_хоста_цо`*`:`*`порт`*`/oc/api/help`

Процедура

1. В строке меню Центра операций установите указатель мыши на значок параметров  и щелкните по Параметры.
2. На странице Общие включите переключатель Включить API REST администрирования.
3. Щелкните по Сохранить.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Конфигурирование для защищенной связи

Центр операций использует протокол HTTPS (Hypertext Transfer Protocol Secure) для связи с Web-браузерами. Протокол Transport Layer Security (TLS) защищает связь между Центром операций и хаб-сервером, а также между хаб-сервером и связанными подчиненными серверами.

Об этой задаче

TLS 1.2 требуется для защищенной связи между сервером IBM Spectrum Protect и компонентом Центр операций, а также между хаб-сервером и подчиненными серверами.

- Защита связи между Центром операций и хаб-сервером
  Для защиты связи между компонентом Центр операций и хаб-сервером нужно добавить сертификат Transport Layer

Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

- Защита связи между хаб-сервером и подчиненным сервером
  Чтобы защитить связь между хаб-сервером и подчиненным сервером с использованием протокола Transport Layer Security (TLS), нужно задать для хаб-сервера сертификат подчиненного сервера и сертификат хаб-сервера - для подчиненного сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.
- Переустановка пароля файла доверенного хранилища Центра операций
  Чтобы настроить защищенную связь между компонентом Центр операций и хаб-сервером, вы должны знать пароль доверенного хранилища компонента Центр операций. Этот пароль создается при установке Центра операций. Если вы не знаете пароль, то вы можете переустановить его.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Защита связи между Центром операций и хаб-сервером

Для защиты связи между компонентом Центр операций и хаб-сервером нужно добавить сертификат Transport Layer Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Прежде чем начать

Файл доверенного хранилища компонента Центр операций - это контейнер сертификатов, доступ к которому может получить Центр операций. Файл доверенного хранилища содержит сертификат, который Центр операций использует для связи HTTPS с веб-браузерами.

При установке Центра операций вы создаете пароль для файла доверенного хранилища. Чтобы защитить связь между компонентом Центр операций и хаб-сервером, нужно использовать тот же пароль для добавления сертификата хаб-сервера в файл доверенного хранилища. Если вы не помните этот пароль, вы можете его переустановить. Смотрите раздел Переустановка пароля файла доверенного хранилища Центра операций.

Процедура

1. Задайте сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера.

   Чтобы указать cert256.arm в качестве сертификата по умолчанию, выполните следующие действия:

   a. Находясь в каталоге экземпляра хаб-сервера, введите следующую команду:

   ```
   gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
    -label "TSM Server SelfSigned SHA Key"
   ```

   b. Перезапустите хаб-сервер, чтобы он получил изменения, внесенные в файл базы данных ключей.
2. Чтобы проверить, задан ли сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера, введите следующую команду:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

3. Остановите веб-сервер Центр операций.
4. Перейдите в командную строку операционной системы, в которой установлен компонент Центр операций.
5. Добавьте сертификат в файл доверенных сертификатов компонента Центр операций, используя утилиту iKeycmd или утилиту iKeyman.

   Утилита iKeyman - это интерфейс командной строки, а утилита iKeyman - это графический пользовательский интерфейс IBM® Key Management.

    Операционные системы AIX  Операционные системы LinuxУтилиты iKeycmd и iKeyman нужно запускать от имени пользователя root.

    Операционные системы WindowsУтилиты iKeycmd и iKeyman должны выполняться от имени учетной записи администратора.

   Чтобы добавить сертификат TLS, используя интерфейс командной строки, выполните следующие шаги:

   a. Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:
      -  Операционные системы AIX  Операционные системы Linux*каталог_установки*/ui/jre/bin

- Операционные системы Windows*каталог_установки*\ui\jre\bin

b. Введите команду iKeycmd, чтобы добавить сертификат cert256.arm в качестве сертификата по умолчанию в файл базы данных ключей хаб-сервера:

```
ikeycmd -cert -add
-db /каталог_установки/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /fvt/comfrey/srv/cert256.arm
-label 'описание метки'
-pw 'пароль' -type jks -format ascii -trust enable
```

Здесь используются следующие обозначения:

каталог_установки
: Каталог установки компонента Центр операций.

описание метки
: Описание, заданное вами для метки.

пароль
: Пароль, созданный вами при установке компонента Центр операций. Чтобы переустановить пароль, деинсталлируйте компонент Центр операций, удалите файл .jks и переустановите компонент Центр операций.

Чтобы добавить сертификат, используя окно IBM Key Management, выполните следующие шаги:

a. Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:
   - Операционные системы AIXОперационные системы Linux*каталог_установки*/ui/jre/bin
   - Операционные системы Windows*каталог_установки*\ui\jre\bin
b. Откройте окно Управление ключами IBM, введя следующую команду:

```
ikeyman
```

c. Выберите Файл базы данных ключей > Открыть.
d. В окне Открыть щелкните по Просмотр и перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен Центр операций:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer
e. Выберите в каталоге guiServer файл gui-truststore.jks.
f. Щелкните по Открыть, а затем по OK.
g. Введите пароль для файла доверенного хранилища и щелкните по OK.
h. В области Контент базы данных ключей окна Управление ключами IBM щелкните по стрелке и выберите в списке Сертификаты подписывающих.
i. Щелкните по Добавить.
j. В окне Открыть щелкните по Обзор и перейдите в каталог экземпляра хаб-сервера, как показано в следующем примере:
   - Операционные системы AIXОперационные системы Linux/opt/tivoli/tsm/server/bin
   - Операционные системы Windowsc:\Program Files\Tivoli\TSM\server1

   В каталоге содержится сертификат cert256.arm.

   Если из окна Открыть недоступен каталог экземпляра хаб-сервера, выполните следующие действия:
   i. При помощи FTP или другого способа передачи файлов скопируйте файлы cert256.arm с хаб-сервера в следующий каталог на компьютере, на котором установлен Центр операций:
      - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
      - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer
   ii. В окне Открыть перейдите в каталогguiServer.
k. Выберите сертификат cert256.arm в качестве сертификата.
   Совет: Выбранный сертификат должен быть задан в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера. Дополнительную информацию смотрите в описании шагов 1 и 2.
l. Щелкните по Открыть, а затем по OK.
m. Введите метку для сертификата. Например, задайте имя хаб-сервера.
n. Щелкните по OK. Сертификат SSL хаб-сервера добавлен в файл доверенного хранилища, и его метка выводится в области Содержимое базы данных ключей окна Управление ключами IBM.
o. Закройте окно Управление ключами IBM.

6. Запустите веб-сервер Центра операций.
7. Когда вы в первый раз будете соединяться с компонентом Центр операций, вас попросят указать IP-адрес или сетевое имя хаб-сервера и номер порта для связи с хаб-сервером. Если опция сервера ADMINONCLIENTPORT включена для сервераIBM Spectrum Protect, введите номер порта, заданный опцией сервера TCPADMINPORT. Если опция сервера ADMINONCLIENTPORT не включена, введите номер порта, заданный опцией сервера TCPPORT. Если компонент Центр операций сконфигурирован, вы можете посмотреть содержимое файла serverConnection.properties, чтобы проверить информацию о соединении. Файл serverConnection.properties находится в следующем каталоге компьютера, где установлен компонент Центр операций:
   -  Операционные системы AIX  Операционные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   -  Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer

Дальнейшие действия

Информацию о настройке связи TLS между хаб-сервером и подчиненным сервером смотрите в разделе Защита связи между хаб-сервером и подчиненным сервером.

Ссылки, связанные с данной:
QUERY OPTION (Запросить информацию о серверных опциях)
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Защита связи между хаб-сервером и подчиненным сервером

Чтобы защитить связь между хаб-сервером и подчиненным сервером с использованием протокола Transport Layer Security (TLS), нужно задать для хаб-сервера сертификат подчиненного сервера и сертификат хаб-сервера - для подчиненного сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.

Об этой задаче

Хаб-сервер получает информацию об оповещениях и состоянии от подчиненного сервера и показывает эту информацию в компоненте Центр операций. Чтобы получить информацию о состоянии и оповещениях от подчиненного сервера, сертификат подчиненного сервера нужно добавить в файл доверенных сертификатов хаб-сервера. Кроме того, нужно сконфигурировать Центр операций для мониторинга подчиненного сервера.

Чтобы включить другие функции компонента Центр операций, например, автоматическое внедрение обновлений клиента, сертификат хаб-сервера нужно добавить в файл доверенных сертификатов подчиненного сервера.

Процедура

1. Выполните следующие шаги, чтобы задать сертификат подчиненного сервера для хаб-сервера:
   a. На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.
   b. Задайте необходимый сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей подчиненного сервера. Введите следующую команду:

      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
       -label "TSM Server SelfSigned SHA Key"
      ```

   c. Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```

   d. Передайте безопасным способом файл cert256.arm подчиненного сервера на хаб-сервер.
   e. На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
   f. Задайте сертификат подчиненного сервера на хаб-сервере. Введите указанную ниже команду в каталоге экземпляра хаб-сервера, где *имя_подчиненного_сервера* - это имя подчиненного сервера, а *подчиненный_cert256.arm* - имя файла сертификата подчиненного сервера:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
       -label имя_подчиненного_сервера -file подчиненный_cert256.arm
      ```

2. Выполните следующие шаги, чтобы задать сертификат хаб-сервера для подчиненного сервера:
   a. На хаб-сервере перейдите в каталог экземпляра хаб-сервера.
   b. Задайте необходимый сертификат cert256.arm в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера. Введите следующую команду:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
 -label "TSM Server SelfSigned SHA Key"
```

c. Проверьте сертификаты в файле базы данных ключей подчиненного сервера. Введите следующую команду:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

d. Передайте безопасным способом файл cert256.arm хаб-сервера на подчиненный сервер.
e. На подчиненном сервере перейдите в каталог экземпляра подчиненного сервера.
f. Задайте сертификат хаб-сервера для подчиненного сервера. Введите указанную ниже команду из каталога экземпляра подчиненного сервера, где *имя_хаб_сервера* - это имя хаб-сервера, а *хаб_cert256.arm* - это имя файла сертификата хаб-сервера:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
 -label имя_хаб_сервера -file хаб_cert256.arm
```

3. Перезапустите хаб-сервер и подчиненный сервер.
4. Выполните следующие шаги, чтобы задать подчиненный сервер для хаб-сервера и хаб-сервер для подчиненного сервера:
   a. Введите на хаб-сервере и на подчиненном сервере следующие команды:

```
SET SERVERPASSWORD пароль_сервера
SET SERVERHLADDRESS ip_адрес
SET SERVERLLADDRESS порт_tcp
```

   b. На хаб-сервере введите команду DEFINE SERVER в соответствии со следующим примером:

```
DEFINE SERVER имя_подчиненного_сервера HLA=адрес_подчиненного_сервера
 LLA=spoke_SSLTCPADMINPort SERVERPA=пароль_подчиненного_сервера
```

   c. На подчиненном сервере введите команду DEFINE SERVER в соответствии со следующим примером:

```
DEFINE SERVER имя_хаб_сервера HLA=адрес_хаба
 LLA=hub_SSLTCPADMINPort SERVERPA=пароль_хаб_сервера
```

   Совет: По умолчанию, взаимодействия с сервером шифруются за исключением случаев, когда сервер отправляет или принимает данные объектов. Данные объектов отправляются и принимаются с использованием TCP/IP. Если выбрать опцию, запрещающую шифровать данные объекта, производительность сервера будет аналогична взаимодействиям в сеансе TCP/IP, и сеанс будет защищен. Чтобы зашифровать все взаимодействия с указанным сервером, даже если сервер отправляет или принимает данные объектов, задайте параметр SSL=YES в команде DEFINE SERVER.
5. Выполните следующие шаги, чтобы сконфигурировать Центр операций для мониторинга подчиненного сервера:
   a. В строке меню компонента Центр операций щелкните по Серверы. Подчиненный сервер будет находиться в состоянии "Без мониторинга". Это состояние означает, что, хотя этот сервер задан для хаб-сервера с использованием команды DEFINE SERVER, сервер еще не сконфигурирован как подчиненный сервер.
   b. Щелкните по подчиненному серверу, чтобы выделить элемент, и щелкните по Отслеживать подчиненный.

Ссылки, связанные с данной:
DEFINE SERVER (Задать сервер для обмена данными между серверами)
QUERY OPTION (Запросить информацию о серверных опциях)
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Переустановка пароля файла доверенного хранилища Центра операций

Чтобы настроить защищенную связь между компонентом Центр операций и хаб-сервером, вы должны знать пароль доверенного хранилища компонента Центр операций. Этот пароль создается при установке Центра операций. Если вы не знаете пароль, то вы можете переустановить его.

Об этой задаче

Чтобы переустановить пароль, нужно создать новый пароль, удалить файл склада доверенных сертификатов компонента Центр операций и перезапустить веб-сервер компонента Центр операций.
Внимание: Выполняйте эти шаги, только если вам неизвестен пароль склада доверенных сертификатов. Не выполняйте эти шаги, если вам известен пароль склада доверенных сертификатов и вы хотите только изменить пароль. Чтобы

переустановить пароль, нужно удалить файл склада доверенных сертификатов; при этом будут удалены все сертификаты, которые уже хранятся в файле склада доверенных сертификатов. Если вам известен пароль склада доверенных сертификатов, вы можете изменить его, используя iKeycmd или утилиту iKeyman.

Процедура

1. Остановите веб-сервер Центр операций.
2. Перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer
3. Откройте файл bootstrap.properties, содержащий пароль файла доверенного хранилища. Если пароль не зашифрован, то вы можете открыть с его помощью файл доверенного хранилища, и переустанавливать пароль не нужно.
   В следующих примерах показана разница между зашифрованным и незашифрованным паролями:

   Пример зашифрованного пароля
   Зашифрованные пароли начинаются со строки `{xor}`.
   В следующем примере показан зашифрованный пароль в качестве значения параметра tsm.truststore.pswd:

   ```
   tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
   ```

   Пример незашифрованного пароля
   В следующем примере показан незашифрованный пароль в качестве значения параметра tsm.truststore.pswd:

   ```
   tsm.truststore.pswd=J8b%^B
   ```

4. Переустановите пароль, заменив пароль в файле bootstrap.properties на новый пароль. Пароль можно заменить на зашифрованный или на незашифрованный пароль. Запомните незашифрованный пароль для последующего использования.
   Чтобы создать зашифрованный пароль, сделайте следующее:
   a. Создайте незашифрованный пароль.
   Пароль для доверенного хранилища должен отвечать следующим критериям:
      - Пароль должен содержать не менее 6 и не более 64 символов.
      - Пароль должен содержать, как минимум, следующие символы:
        - Одну заглавную букву (A – Z)
        - Одну строчную букву (a – z)
        - Одну цифру (0 – 9)
        - Два символа, не являющихся алфавитно-цифровыми, которые указаны в следующем ряду:

          ```
          ~ @ # $ % ^ & * _ - + = ` |

          ( ) { } [ ] : ; < > , . ? /
          ```

   b. В командной строке операционной системы перейдите в следующий каталог:
      - Операционные системы AIXОперационные системы Linux*каталог_установки*/ui/Liberty/bin
      - Операционные системы Windows*каталог_установки*\ui\Liberty\bin
   c. Чтобы зашифровать пароль, введите следующую команду, где *пароль* - это незашифрованный пароль:
      - Операционные системы AIXОперационные системы Linux`securityUtility encode` *пароль* `--encoding=aes`
      - Операционные системы Windows`securityUtility.bat encode` *пароль* `--encoding=aes`

   Операционные системы WindowsМожет появиться следующее сообщение:

   ```
   ! "java" не распознано как внешняя или внутренняя команда,
   программа или пакетный файл.
   ```

   Если появится это сообщение, выполните следующие действия:
      i. Введите следующую команду, где *каталог_установки* - это каталог, куда установлен Центр операций:

      ```
      set JAVA_HOME="каталог_установки\ui\jre"
      ```

      ii. Снова введите следующую команду, чтобы зашифровать пароль:

      ```
      securityUtility.bat encode пароль --encoding=aes
      ```

5. Закройте файл bootstrap.properties.
6. Перейдите в следующий каталог:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer
7. Удалите файл gui-truststore.jks, который является файлом доверенного хранилища Центра операций.
8. Запустите веб-сервер Центра операций.

Результаты

Новый файл доверенного хранилища создается автоматически для компонента Центр операций, и сертификат TLS компонента Центр операций автоматически включается в файл доверенного хранилища.
Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Запуск и остановка веб-сервера

Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.

Процедура

Остановите и перезапустите Web-сервер.

- Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующие команды:
  - Чтобы остановить сервер:

    ```
    ./stopserver.sh
    ```

  - Чтобы запустить сервер:

    ```
    ./startserver.sh
    ```

- Операционные системы LinuxВведите следующие команды:
  - Чтобы остановить сервер:

    ```
    service opscenter.rc stop
    ```

  - Чтобы запустить сервер:

    ```
    service opscenter.rc start
    ```

  - Чтобы перезапустить сервер:

    ```
    service opscenter.rc restart
    ```

  Для определения, запущен ли сервер, введите следующую команду:

  ```
  service opscenter.rc status
  ```

- Операционные системы WindowsВ окне Службы остановите и перезапустите снова службу Центр операций.

Открытие Центра операций

Страница Обзор - это начальное представление по умолчанию в Центре операций. Однако в веб-браузере можно поместить в закладки страницу, которую вы хотите открывать при входе в Центр операций.

Процедура

1. В браузере введите следующий адрес, где *имя_хоста* - это имя компьютера, на котором установлен Центр операций, а *защищенный_порт* - это номер порта, который Центр операций использует для связи HTTPS на этом компьютере:

   ```
   https://имя_хоста:защищенный_порт/oc
   ```

Советы:
   - В URL учитывается регистр символов. Например, убедитесь, что вы ввели "oc" строчными буквами, как это показано.
   - Номер порта по умолчанию для связи HTTPS - 11090, но во время установки Центра операций можно задать другой номер порта.
2. Войдите в систему с ID администратора, который зарегистрирован на хаб-сервере.

   На странице Обзор показана сводная информация для клиентов, служб, серверов, пулов хранения и устройств хранения. Чтобы просмотреть дополнительные сведения, можно щелкнуть по этим элементам или использовать панель меню Центр операций.

   Отслеживание с мобильного устройства: Чтобы удаленно отслеживать среду хранения, можно просматривать страницу Обзор Центр операций в веб-браузере мобильного устройства. Центр операций поддерживает веб-браузер Apple Safari на iPad. Можно использовать и другие мобильные устройства.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Сбор диагностической информации посредством службы управления клиентом Tivoli Storage Manager

служба управления клиентами собирает диагностическую информацию о клиентах резервного копирования и архивирования и делает ее доступной для Центра операций для основных функций мониторинга.

Об этой задаче

После установки службы управления клиентом на странице Диагностика в Центре операций содержится диагностическая информация для клиентов резервного копирования и архивирования.

Диагностическую информацию можно собрать только с клиентов Linux и Windows, но администраторы могут просматривать диагностическую информацию по компоненту Центр операций в операционных системах AIX, Linux или Windows.

Также можно установить компонент служба управления клиентами на узлах перемещения данных для IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, чтобы собирать диагностическую информацию о функциях перемещения данных.

Совет: В документации к службе управления клиентом *компьютер клиента* - это компьютер, на котором установлен клиент резервного копирования и архивирования.

- Установка службы управления клиентом при помощи графического мастера
  Для сбора диагностической информации о клиентах резервного копирования и архивирования (например, файлов журналов клиентов) нужно установить службу управления клиентом на управляемых компьютерах клиентов.
- Установка службы управления клиентом в режиме без вывода сообщений
  Службу управления клиентом можно установить в режиме без вывода сообщений. В режиме без вывода сообщений вы задаете значения установки в файле ответов, а затем запускаете команду установки.
- Проверка правильности установки службы управления клиентом
  Чтобы можно было использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, нужно убедиться, что служба правильно установлена и сконфигурирована.
- Конфигурирование Центра операций для использования службы управления клиентом
  Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, то нужно сконфигурировать Центр операций для доступа к службе управления клиентом.
- Запуск и остановка службы управления клиентом
  Служба управления клиентом автоматически запускается после установки службы на компьютере клиента. В некоторых случаях может понадобиться остановить и запустить службу.
- Удаление службы управления клиентом
  Если вам больше не нужно собирать диагностическую информацию о клиенте, то вы можете деинсталлировать службу управления клиентом с компьютера клиента.
- Конфигурирование службы управления клиентом для пользовательских установок клиента
  Служба управления клиентом использует информацию в файле конфигурации клиента (client-configuration.xml) для обнаружения диагностической информации. Если служба управления клиентами не может обнаружить положение

файлов журнала, то нужно запустить утилиту CmsConfig, чтобы добавить каталог файлов журнала в файл client-configuration.xml.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Установка службы управления клиентом при помощи графического мастера

Для сбора диагностической информации о клиентах резервного копирования и архивирования (например, файлов журналов клиентов) нужно установить службу управления клиентом на управляемых компьютерах клиентов.

Прежде чем начать

Ознакомьтесь с разделом Требования и ограничения для службы управления клиентом.

Об этой задаче

Службу управления клиентом нужно установить на компьютере, на котором установлен клиент резервного копирования и архивирования.

Процедура

1. Скачайте пакет установки компонента служба управления клиентами с такого сайта скачивания IBM®, как IBM Passport Advantage или IBM Fix Central. Ищите имя файла, аналогичное следующему: `<версия>-IBM-SPCMS-<операционная система>.bin`.

   В следующей таблице приведены имена пакетов установки.

Операционная система клиента	Имя пакета установки
Linux x86 64-разрядная	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows 32-разрядная	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows 64-разрядная	8.1.x.000-IBM-SPCMS-Windows64.exe

2. Создайте каталог на компьютере клиента, которым вы хотите управлять, и скопируйте в него пакет установки.
3. Распакуйте контент файла пакета установки.
   - На компьютерах клиента Linux сделайте следующее:
     a. Преобразуйте файл в выполняемый файл; для этого введите следующую команду:

     ```
     chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

     b. Введите следующую команду:

     ```
     ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

   - На компьютерах клиента Windows дважды щелкните по имени пакета установки в Проводнике Windows.

   Совет: Если вы ранее установили и деинсталлировали пакет, то выберите Все, когда вам предложат заменить существующие файлы установки.
4. Запустите пакетный файл установки из каталога, в который вы распаковали файлы установки и связанные файлы. Это каталог, который вы создали на шаге 2.
   - На компьютерах клиента Linux введите следующую команду:

     ```
     ./install.sh
     ```

   - На компьютерах клиента Windows дважды щелкните по install.bat.
5. Для установки службы управления клиентом выполните инструкции в мастере IBM Installation Manager.

   Если продукт IBM Installation Manager не установлен на компьютере клиента, нужно выбрать и IBM Installation Manager, и Службы управления клиентом IBM Spectrum Protect.

   Совет: Можно принять значения по умолчанию для каталога общих ресурсов и каталога установки IBM Installation Manager.

Дальнейшие действия

Следуйте инструкциям в разделе Проверка правильности установки службы управления клиентом.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Установка службы управления клиентом в режиме без вывода сообщений

Службу управления клиентом можно установить в режиме без вывода сообщений. В режиме без вывода сообщений вы задаете значения установки в файле ответов, а затем запускаете команду установки.

Прежде чем начать

Ознакомьтесь с разделом Требования и ограничения для службы управления клиентом.

Распакуйте пакет установки, выполнив инструкции в разделе Установка службы управления клиентом при помощи графического мастера.

Об этой задаче

Службу управления клиентом нужно установить на компьютере, на котором установлен клиент резервного копирования и архивирования.

Каталог input, находящийся в каталоге, в который извлечен пакет установки, содержит следующий пример файла ответов:

install_response_sample.xml

Вы можете использовать пример файла со значениями по умолчанию или настроить его.

Совет: Чтобы настроить пример файла, создайте копию примера файла, переименуйте ее и измените копию.

Процедура

1. Создайте файл ответов на основе файла примера или используйте пример файла ответов install_response_sample.xml.
   В любом случае убедитесь, что в файле ответов указан номер порта для службы управления клиентом. Порт по умолчанию - 9028. Например:

   ```
   <variable name='port' value='9028'/>
   ```

2. Введите команду установки службы управления клиентом и примите лицензию. В каталоге, в который извлечен файл установочного пакета, введите следующую команду, где *файл_ответов* - это полное имя файла ответов:
   На компьютере клиента Linux:

   ```
   ./install.sh -s -input файл_ответов
   -acceptLicense
   ```

   Например:

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
   ```

   На компьютере клиента Windows:

   ```
   install.bat -s -input файл_ответов -acceptLicense
   ```

   Например:

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

Дальнейшие действия

Следуйте инструкциям в разделе Проверка правильности установки службы управления клиентом.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Проверка правильности установки службы управления клиентом

Чтобы можно было использовать службу управления клиентом для сбора диагностической информации о клиенте резервного копирования и архивирования, нужно убедиться, что служба правильно установлена и сконфигурирована.

Процедура

Введите на компьютере клиента в командной строке следующие команды, чтобы посмотреть конфигурацию службы управления клиентом:

- На компьютерах клиента Linux введите следующую команду:

  ```
  каталог_установки_клиента/cms/bin/CmsConfig.sh
  list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- На компьютерах клиента Windows введите следующую команду:

  ```
  каталог_установки_клиента\cms\bin\CmsConfig.bat list
  ```

  где *каталог_установки_клиента* - это каталог установки клиента резервного копирования и архивирования. Например, если используется установка клиента по умолчанию, то введите следующую команду:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Результат выполнения команды выглядит примерно так:

  ```
  Список конфигурации CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Возможности: [LOG_QUERY]
      Путь опций: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Файл журнала: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Если служба управления клиентами правильно установлена и сконфигурирована, то в выходных результатах показан каталог файла журнала ошибок.
Выходной текст извлекается из следующего файла конфигурации:

- На компьютерах клиента Linux:

  ```
  каталог_установки_клиента/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- На компьютерах клиента Windows:

  ```
  каталог_установки_клиента\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
  ```

Если в выходных результатах нет ни одной записи, то нужно сконфигурировать файл client-configuration.xml. Инструкции по конфигурированию этого файла смотрите в разделе Конфигурирование службы управления клиентом для пользовательских установок клиента. Можно использовать команду CmsConfig verify, чтобы проверить, правильно ли создано определение узла в файле client-configuration.xml.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Конфигурирование Центра операций для использования службы управления клиентом

Если вы не использовали для службы управления клиентом конфигурацию по умолчанию, то нужно сконфигурировать Центр операций для доступа к службе управления клиентом.

Прежде чем начать

Убедитесь, что служба управления клиентами установлена и запущена на компьютере клиента.

Проверьте, используется ли конфигурация по умолчанию. Конфигурация по умолчанию не используется в следующих случаях:

- Служба управления клиентом не использует номер порта по умолчанию (9028).
- Для клиента резервного копирования и архивирования не используется IP-адрес, который используется для компьютера клиента резервного копирования и архивирования. Например, другой IP-адрес может использоваться в следующих случаях:
  - В компьютерной системе установлено две сетевые карты. Клиент резервного копирования и архивирования сконфигурирован для взаимодействия с одной сетью, а служба управления клиентами взаимодействует с другой сетью.
  - На компьютере клиента используется DHCP. Поэтому компьютеру клиента динамически назначается IP-адрес, сохраненный на сервере IBM Spectrum Protect во время предыдущей операции клиента резервного копирования и архивирования. При перезагрузке компьютера клиента ему может быть назначен другой IP-адрес. Чтобы Центр операций всегда мог найти компьютер клиента, нужно задать полное имя домена.

Процедура

Чтобы сконфигурировать Центр операций для использования службы управления клиентом, сделайте следующее:

1. Выберите клиента на странице Клиенты Центра операций.
2. Щелкните по Сведения.
3. Щелкните по вкладке Свойства.
4. В поле URL удаленной диагностики раздела Общее укажите URL для службы управления клиентом на компьютере клиента.

   Адрес должен начинаться с `https`. В следующей таблице показаны примеры URL удаленной диагностики.

Тип URL	Пример
С именем хоста DNS и портом по умолчанию (9028)	`https://server.example.com`
С именем хоста DNS и портом не по умолчанию	`https://server.example.com:1599`
С IP-адресом и портом не по умолчанию	`https://192.0.2.0:1599`

5. Щелкните по Сохранить.

Дальнейшие действия

Вы можете получить доступ к диагностической информации о клиенте (например, к файлам журнала клиента) на вкладке Диагностика в Центре операций.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Запуск и остановка службы управления клиентом

Служба управления клиентом автоматически запускается после установки службы на компьютере клиента. В некоторых случаях может понадобиться остановить и запустить службу.

Процедура

- Чтобы остановить, запустить или перезапустить службу управления клиентом на компьютерах клиента Linux, введите следующую команду:
  - Чтобы остановить службу:

    ```
    service cms.rc stop
    ```

  - Чтобы запустить службу:

    ```
    service cms.rc start
    ```

  - Чтобы перезапустить службу:

    ```
    service cms.rc restart
    ```

- На компьютерах клиента Windows откройте окно Службы и остановите, запустите или перезапустите службу IBM Spectrum Protect Client Management Services.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Удаление службы управления клиентом

Если вам больше не нужно собирать диагностическую информацию о клиенте, то вы можете деинсталлировать службу управления клиентом с компьютера клиента.

Об этой задаче

Для деинсталляции службы управления клиентом нужно использовать IBM® Installation Manager. Если вы больше не собираетесь использовать IBM Installation Manager, то его также можно деинсталлировать.

Процедура

1. Деинсталлируйте службу управления клиентом с компьютера клиента:
   a. Откройте IBM Installation Manager:
      - На компьютере клиента Linux перейдите в каталоге установки IBM Installation Manager в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду:

        ```
        ./IBMIM
        ```

      - На компьютере клиента Windows откройте IBM Installation Manager из меню Пуск.

   b. Щелкните по Деинсталлировать.
   c. Выберите Службы управления клиентом IBM Spectrum Protect и нажмите на Далее.
   d. Щелкните по Деинсталлировать и щелкните по Готово.
   e. Закройте окно IBM Installation Manager.
2. Если IBM Installation Manager больше не нужен, то деинсталлируйте его с компьютера клиента:
   a. Откройте мастер деинсталляции IBM Installation Manager:
      - На компьютере клиента Linux перейдите в каталог uninstall IBM Installation Manager (например, /var/ibm/InstallationManager/uninstall) и введите следующую команду:

        ```
        ./uninstall
        ```

      - На компьютере клиента Windows щелкните по Пуск > Панель управления. После этого щелкните по Деинсталляция программ > IBM Installation Manager > Деинсталлировать.

   b. В окне IBM Installation Manager выберите IBM Installation Manager и щелкните по Далее.
   c. Щелкните по Деинсталлировать и щелкните по Готово.

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Конфигурирование службы управления клиентом для пользовательских установок клиента

Служба управления клиентом использует информацию в файле конфигурации клиента (client-configuration.xml) для обнаружения диагностической информации. Если служба управления клиентами не может обнаружить положение файлов журнала, то нужно запустить утилиту CmsConfig, чтобы добавить каталог файлов журнала в файл client-configuration.xml.

- Утилита CmsConfig
  Если вы не используете конфигурацию клиента по умолчанию, вы можете запустить на компьютере клиента утилиту CmsConfig, чтобы обнаружить каталог файлов журнала и добавить его в файл client-configuration.xml. После завершения конфигурирования служба управления клиентами сможет обращаться к файлам журнала клиента и делать их доступными для базовых диагностических функций в компоненте Центр операций.

 Операционные системы AIX  Операционные системы Linux

Устранение неполадок установки Центра операций

Если в процессе установки Центра операций возникает проблема, которую вы не можете решить, вы можете поискать возможное решение в описаниях уже известных проблем.

-  Операционные системы AIXНевозможно запустить графический мастер установки в системе AIX
  Вы устанавливаете Центр операций в системе AIX при помощи графического мастера, и программа установки не запускается.
-  Операционные системы LinuxКитайский, японский или корейский шрифты неправильно выводятся
  Китайский, японский или корейский шрифты неправильно выводятся в компоненте Центр операций в Red Hat Enterprise Linux 5.

 Операционные системы AIX

Невозможно запустить графический мастер установки в системе AIX

Вы устанавливаете Центр операций в системе AIX при помощи графического мастера, и программа установки не запускается.

Решение

На компьютере должны быть установлены файлы RPM, перечисленные в разделе Установка Центра операций при помощи графического мастера. Убедитесь, что эти файлы RPM установлены.

 Операционные системы Linux

Китайский, японский или корейский шрифты неправильно выводятся

Китайский, японский или корейский шрифты неправильно выводятся в компоненте Центр операций в Red Hat Enterprise Linux 5.

Решение

Установите следующие пакеты шрифтов (их можно получить от Red Hat):

- fonts-chinese
- fonts-japanese
- fonts-korean

 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Деинсталляция Центра операций

Центр операций можно деинсталлировать любым из следующих методов: графический мастер, командная строка в режиме консоли или режим без вывода сообщений.

- Деинсталляция Центра операций при помощи графического мастера
  Центр операций можно деинсталлировать при помощи графического мастера IBM® Installation Manager.
- Деинсталляция Центра операций в режиме консоли
  Чтобы деинсталлировать Центр операций из командной строки, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметр для режима консоли.
- Деинсталляция Центра операций в режиме без вывода сообщений
  Чтобы деинсталлировать Центр операций в режиме без вывода сообщений, запустите программу деинсталляции IBM Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Деинсталляция Центра операций при помощи графического мастера

Центр операций можно деинсталлировать при помощи графического мастера IBM® Installation Manager.

Процедура

1. Откройте IBM Installation Manager.
   Операционные системы AIXОперационные системы LinuxВ каталоге, в котором установлен IBM Installation Manager, перейдите в подкаталог eclipse (например, /opt/IBM/InstallationManager/eclipse) и введите следующую команду:

   ```
   ./IBMIM
   ```

   Операционные системы WindowsОткрыть IBM Installation Manager можно из меню Пуск.
2. Щелкните по Деинсталлировать.
3. Выберите опцию для Центр операций и нажмите на Далее.
4. Щелкните по Деинсталлировать.
5. Щелкните по Готово.

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Деинсталляция Центра операций в режиме консоли

Чтобы деинсталлировать Центр операций из командной строки, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметр для режима консоли.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы AIXОперационные системы Linuxeclipse/tools
   - Операционные системы Windowseclipse\tools

   Например:

   - Операционные системы AIXОперационные системы Linux/opt/IBM/InstallationManager/eclipse/tools
   - Операционные системы WindowsC:\Program Files\IBM\Installation Manager\eclipse\tools
2. В каталоге tools введите следующую команду:
   - Операционные системы AIXОперационные системы Linux`./imcl -c`
   - Операционные системы Windows`imcl.exe -c`
3. Для деинсталляции введите `5`.
4. Выберите деинсталляцию в группе пакетов IBM Spectrum Protect.
5. Введите `N` (Next - Далее).
6. Выберите деинсталляцию пакета компонента Центр операций.
7. Введите `N` (Next - Далее).

8. Введите `U` (Uninstall - Деинсталляция).
9. Введите `F` (Finish - Готово).

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Деинсталляция Центра операций в режиме без вывода сообщений

Чтобы деинсталлировать Центр операций в режиме без вывода сообщений, запустите программу деинсталляции IBM® Installation Manager из командной строки, указав параметры для режима без вывода сообщений.

Прежде чем начать

Вы можете использовать файл ответов, чтобы задать входные данные для деинсталляции сервера Центр операций в режиме без вывода сообщений. IBM Spectrum Protect содержит пример файла ответов, uninstall_response_sample.xml, в каталоге input в том месте, куда был распакован пакет установки. Этот файл содержит значения по умолчанию, которые помогут вам избежать ненужных предупреждений.

Чтобы деинсталлировать Центр операций, оставьте заданное значение `modify="false"` для записи Центр операций в файле ответов.

Если вы хотите настроить файл ответов, вы можете изменить опции, содержащиеся в файле. Информацию о файлах ответов смотрите в разделе Файлы ответов.

Процедура

1. В каталоге, в котором установлен IBM Installation Manager, перейдите в следующий подкаталог:
   - Операционные системы AIXОперационные системы Linuxeclipse/tools
   - Операционные системы Windowseclipse\tools

   Например:

   - Операционные системы AIXОперационные системы Linux/opt/IBM/InstallationManager/eclipse/tools
   - Операционные системы WindowsC:\Program Files\IBM\Installation Manager\eclipse\tools
2. В каталоге tools введите следующую команду, где *файл_ответов* - это полное имя файла ответов:
   - Операционные системы AIXОперационные системы Linux`./imcl -input` *`файл_ответов`* `-silent`
   - Операционные системы Windows`imcl.exe -input` *`файл_ответов`* `-silent`

   Пример команды:
   - Операционные системы AIXОперационные системы Linux`./imcl -input /tmp/input/uninstall_response.xml -silent`
   - Операционные системы Windows`imcl.exe -input C:\tmp\input\uninstall_response.xml -silent`

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Откат к предыдущей версии Центра операций

По умолчанию IBM® Installation Manager сохраняет предыдущие версии пакетов для выполнения отката, если с более поздними версиями обновлений, исправлений или пакетов возникает проблема.

Прежде чем начать

Функция отката доступна только после обновления Центра операций.

Об этой задаче

Если IBM Installation Manager выполняет откат пакета до предыдущей версии, то текущая версия файлов пакета деинсталлируется, а более ранняя версия переустанавливается.

Чтобы выполнить откат к предыдущей версии Центра операций, IBM Installation Manager необходим доступ к файлам для этой версии. По умолчанию эти файлы сохраняются при каждой очередной установке. Поскольку число сохраненных файлов увеличивается с каждой установленной версией, вам может потребоваться удалять эти файлы из системы в соответствии с расписанием. Однако если вы удаляете эти файлы, вы не сможете выполнить откат на предыдущую версию.

Чтобы удалить сохраненные файлы или изменить ваши предпочтения относительно сохранения этих файлов в будущих установках, выполните следующие действия:

1. В IBM Installation Manager выберите Файл > Предпочтения.
2. На странице Предпочтения щелкните по Файлы для отката и укажите свои предпочтения.

Процедура

Чтобы выполнить откат к предыдущей версии Центра операций, используйте функцию Откат программы IBM Installation Manager.

Конфигурирование серверов

Чтобы выполнить задачи по конфигурированию для сервера IBM Spectrum Protect, ознакомьтесь с доступной документацией.

Об этой задаче

Совет: Начиная с IBM® Tivoli Storage Manager версии 7.1.3, публикация *Руководство администратора* в формате PDF не предоставляется. Вместо этого набор документации был исправлен, чтобы помочь вам выполнять отдельные задачи:

- Чтобы реализовать новое решение по защите данных, смотррите раздел Решения по защите данных IBM Spectrum Protect. В руководствах по решению приводятся инструкции типа справочника, которые помогут вам спланировать, реализовать решение и управлять им.
- Либо можно использовать IBM Spectrum Protect Blueprints. Можно выполнить процедуры Blueprint, чтобы внедрить среду хранения, и использовать сценарии Blueprint, чтобы наладить процесс установки и конфигурирования. В Blueprints содержатся самые последние требования к оборудованию и программам для мелких, средних и крупных сред хранения.
- Чтобы администрировать *существующее* решение, смотрите следующую таблицу.

Действие	**Подробности**	**Документация**
Защитите сервер.	Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.	Защита сервера IBM Spectrum Protect
Узнайте о политиках хранения данных и сконфигурируйте их.	Политики IBM Spectrum Protect определяют правила управления вашими данными.	Чтобы обновить политики, используйте компонент Центр операций. Чтобы больше узнать о политиках и создать политики, смотрите раздел Настройка политик.
Устраните дубликаты данных.	Используйте дедупликацию данных, чтобы устранить лишние данные в пулах хранения. Дедупликация данных сокращает объем пространства, который требуется для хранения данных. В дедуплицированном пуле хранения на носителе сохраняется только один экземпляр данных. При работе с IBM Spectrum Protect V7.1.3 и новее можно использовать встроенную дедупликацию данных.	Чтобы подробнее узнать о различиях между встроенной дедупликацией данных и дедупликацией данных после обработки, а также сконфигурировать наилучшее практическое решение по дедупликации данных, смотрите раздел Опции дедупликации данных.

Действие	Подробности	Документация
Реплицируйте данные.	Вы можете реплицировать данные клиентского узла с исходного сервера репликации на целевой сервер репликации. Если произойдет авария и сервер источника временно окажется недоступен, то клиентские узлы смогут восстановить свои данные с целевого сервера репликации.	Чтобы реализовать наилучшее практическое решение, в котором используется репликация IBM Spectrum Protect и автоматическая передача управления при отказе, смотрите раздел Дисковое решение для нескольких площадок. Общую информацию о репликации, включая шаги по конфигурированию, смотрите в разделе Репликация данных клиента на другой сервер.
Отслеживайте решение по хранению.	Отслеживайте решение по хранению, чтобы выявить существующие и потенциальные проблемы. Таким образом вы сможете устранять ошибки и оптимизировать производительность системы.	Мониторинг решений по хранению
Управляйте базой данных и журналом восстановления.	В базе данных и в журнале восстановления или в перечне сервера хранится информация о данных клиента, и они являются критически важными для работы сервера.	• Общую информацию о базе данных и журнале восстановления смотрите в разделе Управление базой данных и журналом восстановления (V7.1.1). • Чтобы узнать, как оптимизировать реорганизацию индекса и таблиц для базы данных сервера и избежать неожиданных проблем, связанных с ростом базы данных и производительностью, и устранить эти проблемы, смотрите раздел Техническое замечание 1683633.
Сконфигурируйте SSL для Lightweight Directory Access Protocol (LDAP).	Вы можете сконфигурировать SSL для серверов каталога LDAP и управлять паролями и процедурами входа в систему.	Информацию об LDAP смотрите в следующих источниках: • Аутентификация пользователей с использованием сервера LDAP • Конфигурирование SSL или TLS для серверов каталогов LDAP (V7.1.1)

Действие	Подробности	Документация
Защитите сервер и произведите восстановление при аварии.	Защитите инфраструктуру вашей системы и данные, чтобы иметь возможность произвести восстановление в случае аварии. Используйте инструменты и процедуры, обеспечиваемые продуктом IBM Spectrum Protect - это поможет вам создать план действий при аварии.	Информацию о защите и восстановлении сервера и данных смотрите в следующих источниках: • Защита базы данных и файлов настройки инфраструктуры (V7.1.1) • Использование менеджера аварийного восстановления для ленточных сред (V7.1.1) • Восстановление данных
Защитите клиенты.	Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.	Конфигурирование клиентов для приложений, виртуальных машин и компьютеров
Выберите и сконфигурируйте пространство хранения.	Выберите хранение, исходя из ваших бизнес-требований, а затем выполните задачи по конфигурированию.	Конфигурирование хранения
Защитите файл-серверы NAS.	Вы можете спланировать, сконфигурировать и управлять средой резервного копирования, которая защищает ваш файл-сервер NAS (Network-Attached Storage).	Защита файл-серверов NAS
Сконфигурируйте кластерную среду.	Сконфигурируйте кластерную среду в операционных системах AIX, Linux или Windows, чтобы обеспечить высокую доступность сервера и сведенное к минимуму время простоя.	Конфигурирование кластерных сред
Сконфигурируйте виртуальные ленточные библиотеки.	Виртуальная ленточная библиотека (Virtual Tape Library, VTL) не использует физические ленточные носители. При реализации хранилища VTL вы не ограничены емкостью физической ленточной библиотеки. Возможность определения многих томов и накопителей может обеспечить большую гибкость для среды хранения.	Конфигурирование виртуальных ленточных библиотек
Защитите данные с использованием лицензированной функции NetApp SnapLock.	Лицензированную функцию NetApp SnapLock можно использовать, чтобы выполнить строгие нормативные требования для заархивированных данных.	Защита данных с использованием лицензированной функции NetApp SnapLock

Действие	Подробности	Документация
Управляйте операциями.	Управляйте операциями серверов и клиентов, чтобы избежать потенциальных проблем и повысить производительность.	Управление операциями

- Защита сервера IBM Spectrum Protect
  Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.
- Репликация данных клиента на другой сервер
  Репликация данных клиента с исходного сервера на другой сервер помогает убедиться, что в случае повреждения исходного сервера для восстановления будет доступна резервная копия данных клиента. При репликации производится инкрементное копирование данных с исходного сервера на сервер назначения, чтобы обеспечить возможность передачи управления в случае отказа и возврата управления.
- Конфигурирование кластерных сред
  Сервер IBM Spectrum Protect можно сконфигурировать для кластеризации в системах AIX, Linux или Windows.

Защита сервера IBM Spectrum Protect

Защитите сервер IBM Spectrum Protect и данные, управляя доступом к серверам и клиентским узлам, шифруя данные и обеспечивая защищенные уровни прав доступа и пароли.

- Понятия, касающиеся защиты
  Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.
- Управление администраторами
  Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.
- Изменение требований к паролям
  Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.
- Защита IBM Spectrum Protect в системе
  Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.
- Защита среды хранения против программ-вымогателей
  Среды хранения, подключенные к Интернету, могут быть целью атак программ-вымогателей. Можно выполнить шаги, чтобы помочь защитить среду хранения от программ, требующих выкуп, и убедиться, что вы сможете восстановить серверы и клиенты, если произойдет атака.
- Защита связи
  Ваши данные и пароли будут более защищены, если они защищены с использованием Secure Sockets Layer (SSL) или Transport Layer Security (TLS), форма SSL.
- Аутентификация пользователей IBM Spectrum Protect с использованием сервера LDAP
  В системе IBM Spectrum Protect пользователи должны аутентифицироваться на сервере, вводя ID пользователя и пароль. Если ваша организация использует для управления ID пользователей сервер Lightweight Directory Access Protocol (LDAP), можно с помощью сервера LDAP аутентифицировать ID пользователей IBM Spectrum Protect.

Понятия, касающиеся защиты

Вы можете защитить IBM Spectrum Protect от рисков защиты, используя протоколы связи, защиту паролей и предоставляя администраторам разные уровни доступа.

Transport Layer Security

Можно использовать протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS), чтобы обеспечить защиту транспортного слоя для безопасной связи между серверами, клиентами и агентами хранения. Если вы пересылаете данные между сервером, клиентом и агентом хранения, используйте SSL или TLS для шифрования данных.

Совет: Любая документация IBM Spectrum Protect, обозначенная как "SSL" или "выбрать SSL", применима к TLS.

SSL предоставляется Global Security Kit (GSKit), установленным с сервером IBM Spectrum Protect и используемым сервером, клиентом и агентом хранения.

Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных DB2, который используется какими-либо серверами IBM Spectrum Protect.

Каждый сервер, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатором (certificate authority, CA). Вы можете использовать свои собственные сертификаты или можете приобрести сертификаты у сертификатора (CA). Любой сертификат нужно установить и добавить к базе данных ключей для сервера IBM Spectrum Protect, клиента или агента хранения. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL. Некоторые сертификаты сертификаторов предварительно устанавливаются в базах данных ключей по умолчанию.

SSL устанавливается независимо от сервера IBM Spectrum Protect, клиента и агента хранения.

Уровни полномочий

При использовании каждого сервера IBM Spectrum Protect существует ряд доступных уровней административных полномочий, определяющих задачи, которые может выполнить администратор.

После регистрации администратору нужно предоставить полномочия, назначив для него один или несколько уровней административных полномочий. Администратор с системными полномочиями может выполнить любую задачу с сервером и назначить уровни полномочий для других администраторов, воспользовавшись командой GRANT AUTHORITY. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Администратор может зарегистрировать другие ID администраторов, предоставить им уровни полномочий, переименовать или удалить их, а также блокировать или разблокировать их доступ к серверу.

Администратор может управлять доступом к определенным клиентским узлам для ID пользователей root и ID пользователей, не являющихся пользователями root. По умолчанию, ID пользователя, не являющегося пользователем root, не может производить резервное копирование данных на узле. Используйте команду UPDATE NODE, чтобы изменить параметры узла и включить резервное копирование.

Пароли

По умолчанию сервер автоматически использует аутентификацию с помощью пароля. Если аутентификация пароля включена (on), все пользователи при получении доступа к серверу должны указывать пароль.

Используйте Lightweight Directory Access Protocol (LDAP), чтобы применить более строгие требования к паролям. Дополнительную информацию смотрите в разделе Аутентификация пользователей с использованием сервера LDAP.

Табл. 1. Характеристики аутентификации паролей

Характеристика	**Дополнительная информация**
Значение регистра символов	Без учета регистра.
Срок действия пароля по умолчанию	90 дней. Отсчет начинается с момента первой регистрации на сервере ID администратора или клиентского узла. Если в течение этого периода пароль не изменится, пароль нужно будет изменить, когда пользователь в следующий раз получит доступ к серверу.
Число попыток ввода неправильного пароля	Для всех клиентских узлов можно установить максимальное количество последовательных попыток неправильного ввода пароля. После превышения данного значения сервер блокирует такой узел.
Длина пароля по умолчанию	8 символов Администратор может задать минимальную длину. Начиная с версии 8.1.4, минимальная длина паролей сервера по умолчанию изменилась с 0 до 8 символов.

Защита сеанса

Защита сеанса - это уровень защиты, который используется для взаимодействий между узлами-клиентами IBM Spectrum Protect, клиентами администрирования и серверами и назначается с использованием параметра SESSIONSECURITY.

Для параметра SESSIONSECURITY можно задать одно из следующих значений:

- Значение STRICT принудительно применяет наиболее высокий уровень защиты взаимодействий между серверами IBM Spectrum Protect, узлами и администраторами.
- Значение TRANSITIONAL указывает, что при обновлении программы IBM Spectrum Protect до V8.1.2 или новее используется существующий протокол связи. Это значение по умолчанию. Если задано SESSIONSECURITY=TRANSITIONAL, автоматически применяются более строгие параметры защиты при использовании более высоких версий протокола TLS и при обновлении программы до V8.1.2 или новее. После того как узел, администратор или сервер будет соответствовать требованиям для значения STRICT, защита сеанса автоматически обновится до значения STRICT, и объект больше не сможет проходить аутентификацию, исплользуя предыдущую версию клиента или более ранние протоколы TLS.
  Прим.: До обновления серверов обновлять клиенты резервного копирования и архивирования до V8.1.2 или новее не нужно. После обновления сервера до V8.1.2 или новее узлы и администраторы, использующие более ранние версии программы, продолжат взаимодействовать с сервером, используя значение TRANSITIONAL, пока объект будет соответствовать требованиям для значения STRICT. Точно так же можно обновить клиенты резервного копирования и архивирования до V8.1.2 или новее до обновления серверов IBM Spectrum Protect, но обновлять серверы сначала не требуется. Связь между серверами и клиентами не прерывается.

Дополнительные сведения о значениях параметра SESSIONSECURITY смотрите в описаниях следующих команд.

Табл. 2. Команды, используемые, чтобы задать параметр SESSIONSECURITY

Объект	**Команда**
Клиентские узлы	• REGISTER NODE • UPDATE NODE
Администраторы	• REGISTER ADMIN • UPDATE ADMIN
Серверы	• DEFINE SERVER • UPDATE SERVER

Администраторы, прошедшие аутентификацию с использованием команды DSMADMC, команды DSMC или программы dsm, после аутентификации с использованием V8.1.2 или новее не смогут проходить аутентификацию с использованием более ранней версии. Чтобы устранить проблемы аутентификации администраторов, смотрите следующие советы:
Советы:

- Убедитесь, что все программы IBM Spectrum Protect, используемые учетной записью администратора для входа в систему, обновлены до V8.1.2 или новее. Если учетная запись администратора производит вход из нескольких систем, убедитесь, что сертификат сервера установлен в каждой системе.
- После того как администратор пройдет аутентификацию на сервере V8.1.2 или новее, используя клиент V8.1.2 или новее, администратор сможет проходить аутентификацию только на клиентах или серверах, использующих V8.1.2 или новее. Команду администратора можно вводить из любой системы.
- Если потребуется, создайте отдельную учетную запись администратора, чтобы использовать ее только при работе с клиентами и серверами, на которых работает V8.1.1 или более ранняя программа.

Принудительно примените наивысший уровень защиты взаимодействий с сервером IBM Spectrum Protect, сделав так, чтобы все узлы, администраторы и серверы использовали защиту сеанса STRICT. Можно воспользоваться командой SELECTЮ чтобы определить, какие серверы, узлы и администраторы используют защиту сеанса TRANSITIONAL, чтобы их обновить для использования защиты сеанса STRICT.

Ссылки, связанные с данной:
Защита связи
SELECT (Выполнение запроса SQL базы данных)

Управление администраторами

Администратор с системными полномочиями может выполнить любую задачу с сервером IBM Spectrum Protect, включая назначение уровней полномочий для других администраторов. Чтобы выполнить ряд задач, вам должны быть предоставлены полномочия путем назначения одного или нескольких уровней полномочий.

Процедура

Чтобы изменить параметры администратора, выполните описанные ниже шаги.

Задача	Процедура

Добавить администратора	Чтобы добавить администратора, ADMIN1, с системными полномочиями и задать пароль, выполните следующие шаги:
	a. Зарегистрируйте администратора и задайте Pa$#$twO в качестве пароля, введя следующую команду:
	`register admin admin1 Pa$#$twO`
	b. Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`

Изменить административные полномочия	Измените уровень полномочий для администратора ADMIN1.
	• Предоставьте администратору системные полномочия, введя следующую команду:
	`grant authority admin1 classes=system`
	• Аннулируйте системные полномочия администратора, введя следующую команду:
	`revoke authority admin1 classes=system`

Удалить администраторов	Аннулируйте для администратора ADMIN1 доступ к серверу IBM Spectrum Protect, введя следующую команду: `remove admin admin1`
Временно запретите доступ к серверу	Заблокируйте или разблокируйте администратора, введя команду LOCK ADMIN или UNLOCK ADMIN.

Изменение требований к паролям

Можно изменить минимальный предел пароля, длину пароля, срок действия пароля, а также включить или выключить аутентификацию для IBM Spectrum Protect.

Об этой задаче

Применяя аутентификацию на основе паролей и управляя ограничениями паролей, вы защищаете данные и серверы от потенциальных угроз безопасности.

Процедура

Чтобы изменить требования к паролям для серверов IBM Spectrum Protect, выполните описанные ниже задачи.

Табл. 1. Задачи по аутентификации для серверов IBM Spectrum Protect

Задача	Процедура

Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число неудачных попыток в поле Предел неудачных попыток входа в систему. Значение по умолчанию при установке равно 0.
Задайте минимальную длину пароля.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте число символов в поле Минимальная длина пароля.
Задайте срок действия паролей.	a. Выберите сервер на странице Серверы Центра операций. b. Щелкните по Сведения, а затем по вкладке Свойства. c. Задайте срок в днях в поле Общий срок действия паролей.
Отключите аутентификацию на основе паролей.	По умолчанию сервер автоматически использует аутентификацию с помощью пароля. При аутентификации пароля все пользователи для получения доступа к серверу должны вводить пароль. Запретить аутентификацию пароля можно только для паролей, аутентификация которых выполняется на сервере (LOCAL). Отключая аутентификацию на основе паролей, вы делаете сервер доступным для угроз безопасности.

Задать метод аутентификации по умолчанию.	Введите команду SET DEFAULTAUTHENTICATION. Например, чтобы использовать сервер как метод аутентификации по умолчанию, введите следующую команду:
	
	`set defaultauthentication local`
	
	Чтобы обновить клиентский узел для аутентификации на сервере, включите `AUTHENTICATION=LOCAL` в команду UPDATE NODE:
	
	`update node authentication=local`

Защита IBM Spectrum Protect в системе

Защитите систему, в которой сервер IBM Spectrum Protect работает, чтобы предотвратить несанкционированный доступ.

Процедура

Убедитесь, что неавторизованные пользователи не могут получить доступ к каталогам для базы данных сервера и экземпляра сервера. Оставьте для этих каталогов параметры доступа, которые вы сконфигурировали во время реализации.

- Ограничение доступа пользователей к серверу
  Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

- Ограничение доступа путем ограничений портов
  Ограничьте доступ к серверу, применив ограничения портов.

Ограничение доступа пользователей к серверу

Уровни полномочий определяют то, что администратор может сделать с сервером IBM Spectrum Protect. Администратор с системными полномочиями может выполнить любую задачу на сервере. Администраторы, обладающие полномочиями политики, хранения или оператора, могут выполнять только определенный набор задач.

Процедура

1. После регистрации администратора с использованием команды REGISTER ADMIN используйте команду GRANT AUTHORITY, чтобы задать уровень полномочий администратора. Дополнительные сведения о том, как задавать и изменять полномочия, смотрите в разделе Управление администраторами.
2. Чтобы управлять полномочиями администратора на выполнение некоторых задач, используйте следующие две опции сервера:
   a. Вы можете задать уровень полномочий, который должен быть у администратора, чтобы он мог ввести команды QUERY и SELECT с опцией сервера QUERYAUTH. По умолчанию, не требуется никакого уровня полномочий. Данное требование можно изменить, указав один из уровней полномочий, включая системные.
   b. Вы можете указать, что для команд, которые заставляют сервер записывать внешний файл за счет использования серверной опции REQSYSAUTHOUTFILE, требуются системные полномочия. По умолчанию, для выполнения таких команд необходимы системные полномочия.
3. Можно ограничить резервное копирование данных на клиентском узле, так чтобы его могли выполнять только ID пользователя root или авторизованные пользователи. Например, чтобы ограничить резервное копирование ID пользователя root, введите команду REGISTER NODE или UPDATE NODE и задайте параметр BACKUPINITIATION=root:

```
update node backupinitiation=root
```

Ограничение доступа путем ограничений портов

Ограничьте доступ к серверу, применив ограничения портов.

Об этой задаче

В зависимости от ваших требований к защите вам может потребоваться ограничить доступ к отдельным серверам. Сервер IBM Spectrum Protect можно настроить на прием данных с четырех портов TCP/IP: двух - для обычных протоколов TCP/IP или протоколов Secure Sockets Layer (SSL)/Transport Layer Security (TLS), и двух, которые можно использовать только для протокола SSL/TLS.

Процедура

Чтобы указать нужные порты, можно задать опции сервера (смотрите раздел Табл. 1).

Табл. 1. Опции сервера и доступ к портам

Серверный параметр	Доступ к портам
TCPPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для отслеживания требований установления сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. Значение по умолчанию - 1500.
TCPADMINPORT	Задает номер порта, который используется драйвером связи TCP/IP сервера для ожидания требований установления сеансов, отличных от сеансов клиентов. Этот порт принимает как сеансы TCP/IP, так и сеансы с поддержкой SSL. По умолчанию используется значение, заданное опцией TCPPORT. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.
SSLTCPPORT	Задает адрес порта TCP/IP SSL для сервера. Этот порт принимает только сеансы с поддержкой SSL. Значения порта по умолчанию нет.

Серверный параметр	Доступ к портам
SSLTCPADMINPORT	Задает адрес порта, на котором драйвер связи TCP/IP сервера ожидает требования на установление сеансов SSL. Значения порта по умолчанию нет. Используйте эту опцию, чтобы отделить трафик клиента администрирования от трафика обычных клиентов с опциями TCPPORT и SSLTCPPORT.

ограничения:
Следующие ограничения применяются при определении портов сервера только для SSL (SSLTCPPORT и SSLTCPADMINPORT):

- Если вы задаете порт сервера только SSL в параметре LLADDRESS в команде DEFINE SERVER или UPDATE SERVER, надо также задать параметр SSL=Yes.
- Если вы задаете порт сервера только SSL для опции TCPPORT клиента, то надо также задать YES для опции SSL клиента.

Защита среды хранения против программ-вымогателей

Среды хранения, подключенные к Интернету, могут быть целью атак программ-вымогателей. Можно выполнить шаги, чтобы помочь защитить среду хранения от программ, требующих выкуп, и убедиться, что вы сможете восстановить серверы и клиенты, если произойдет атака.

Об этой задаче

Программа, требующая выкуп - это вредоносная программа, используемая для получения доступа к вычислительной системе и шифровки данных. Как правило, инициатором атаки программы, требующей выкуп, шифрует данные, а затем связывается с владельцем данных, требуя выкуп. Если выкуп не будет выплачен, инициатор атаки угрожает оставить данные зашифрованными. Поэтому вы можете помочь защитить среду хранения от атаки программы, требующей выкупа, сохранив копию данных в расположении, которое *недоступно* из Интернета.

Одна из возможностей - это создание резервной копии вашей базы данных на ленте и резервное копирование клиентов в пулы хранения копий на ленте, а затем перенос ленточных томов в защищенное расположение вне сайта (площадки). Используя такую стратегию, вы сможете включить функцию IBM Spectrum Protect disaster recovery manager (DRM) для отслеживания перемещения носителей вне площадки и регистрации этой информации в базе данных IBM Spectrum Protect. DRM объединяет планы, сценарии и другую информацию в файле плана. Файл плана можно использовать для восстановления серверов и клиентов после атаки программы, требующей выкуп.

Процедура

1. При планировании среды хранения продумайте, нужно ли использовать ленту в качестве носителя хранения и нужно ли перевозить ленточные тома вне площадки. Инструкции по настройке ленточного хранения смотрите в разделе Ленточное решение.
2. При планировании среды хранения продумайте, нужно ли использовать функцию DRM, чтобы это помогло вам произвести восстановление после атаки программы, требующей выкупа, незапланированного отключения или аварии. Введение в DRM смотрите в разделе Подготовка к аварии и восстановление после аварии с использованием DRM.
3. Ознакомьтесь с политикой, заданной для вашей среды хранения, чтобы убедиться, что сохраняется достаточно резервных копий и что копии хранятся в течение достаточного числа дней. Если самые новые ваши файлы будут зашифрованы программой, требующей выкупа, вы все равно сможете получить доступ к предыдущим версиям. Чтобы настроить политику, используйте Центр операций или команды DEFINE COPYGROUP и UPDATE COPYGROUP. Информацию о предпочтительных параметрах смотрите в разделе Хранение версий резервных копий и окончание их действия.
4. Ежедневно отслеживайте систему, чтобы как можно скорее обнаружить программу, требующую выкуп. Дополнительные сведения смотрите в разделах Контрольный список ежедневного мониторинга и Контрольный список периодического мониторинга.

Защита связи

Ваши данные и пароли будут более защищены, если они защищены с использованием Secure Sockets Layer (SSL) или Transport Layer Security (TLS), форма SSL.

SSL и TLS — это стандартная технология создания зашифрованных сеансов между серверами и клиентами. SSL и TLS предоставляют безопасный канал для связи серверов и клиентов по открытым путям связи. При использовании SSL и TLS идентификационная информация сервера проверяется с помощью цифровых сертификатов.

Чтобы защитить вашу среду хранения от угроз защите, серверы, клиенты и агенты хранения, которые используют программу IBM Spectrum Protect V8.1.4 или новее, автоматически конфигурируются для взаимодействий друг с другом с использованием протокола Transport Sockets Layer (TLS) 1.2, и самоподписанные сертификаты распределяются автоматически.
Ограничения, касающиеся более ранних выпусков:

- Начиная с IBM Spectrum Protect V8.1.2, поддержка SSL по умолчанию включена для взаимодействий между серверами и клиентами V8.1.2 и новее. Надо вручную сконфигурировать агенты хранения V8.1.2 для использования SSL.
- Агенты хранения, использующие программу V7.1.8 или новее либо V8.1.3 или новее, автоматически конфигурируются для использования SSL.

  Клиенты библиотеки и серверы менеджеров библиотеки автоматически используют SSL для взаимодействий с агентами хранения, использующими программу V8.1.2 или новее либо V7.1.8 или новее, но вы должны вручную сконфигурировать сертификаты для взаимодействий между ними. Агент хранения автоматически обменивается сертификатами со своим сервером базы данных.

- Начиная с IBM Spectrum Protect™ версии 8.1.4, вам больше не нужно вручную конфигурировать сертификаты между агентами хранения, клиентами библиотек и серверами менеджеров библиотек. Сертификаты конфигурируются автоматически.
- Серверы, агенты хранения и клиенты, которые используют программу IBM Spectrum Protect более ранней версии, чем V8.1.2, или версии программы Tivoli Storage Manager, более ранние, чем V7.1.8, всегда нужно конфигурировать вручную для использования SSL, даже если сервер или агент хранения используют программу V8.1.3 или новее.

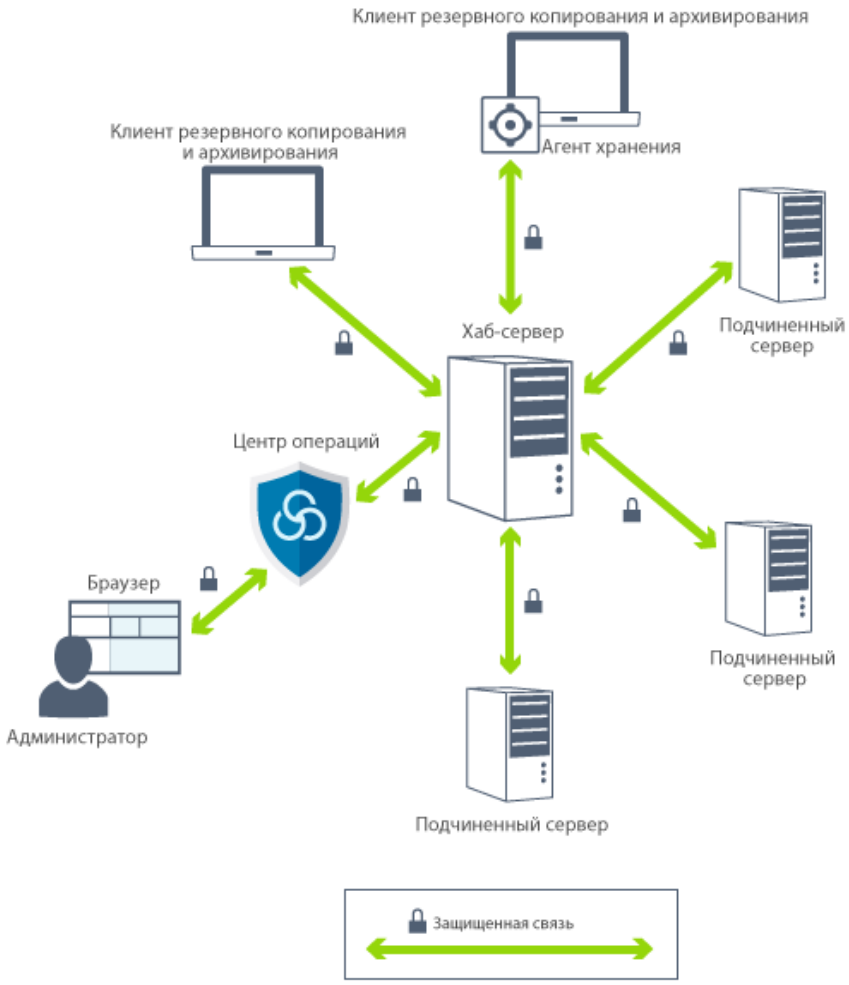
TLS используется для всех взаимодействий между сервером, агентами хранения и клиентами, кроме отправки или получения данных объектов. По умолчанию данные объектов отправляются и принимаются с использованием TCP/IP. Чтобы повысить производительность системы, используйте TLS для аутентификации без шифрования данных объектов. Если выбрать опцию, запрещающую шифровать данные объекта, производительность сервера будет аналогична взаимодействиям в сеансе TCP/IP, и сеанс будет защищен. Чтобы указать, использует ли сервер TLS 1.2 для всего сеанса или только для аутентификации, смотрите описание опции клиента SSL для взаимодействий клиента с сервером и параметра SSL в команде UPDATE SERVER для взаимодействий сервера с сервером. Если вы решите использовать TLS для шифрования данных объектов, рассмотрите возможность добавления дополнительных процессорных ресурсов на сервер IBM Spectrum Protect, чтобы справиться с повышенной нагрузкой процессора.

Если вы используете аутентификацию пароля при помощи сервера каталогов LDAP, TLS защищает пароли при передаче между сервером IBM Spectrum Protect и сервером LDAP. TLS требуется для всех конфигураций обмена паролями LDAP. Сертификаты для серверов каталога LDAP нужно сконфигурировать вручную и добавить в базы данных ключей сервера. Добавлять сертификаты в базы данных ключей агентов хранения не нужно.

- Связь по протоколу Secure Sockets Layer и Transport Layer Security
  Протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS) используется, чтобы обеспечить защиту на уровне транспорта для безопасной связи между серверами, клиентами, агентами хранения IBM Spectrum Protect и компонентом Центр операций. Если вы пересылаете данные между сервером, клиентом и агентом хранения, для шифрования данных используется SSL или TLS.
- Конфигурирование агентов хранения, серверов, клиентов и центра операций для соединения с сервером с использованием SSL
  Сконфигурируйте Secure Sockets Layer (SSL) на сервере IBM Spectrum Protect, на клиенте резервного копирования и архивирования, на агенте хранения и в компоненте Центр операций, чтобы убедиться, что данные при взаимодействиях шифруются.

Связь по протоколу Secure Sockets Layer и Transport Layer Security

Протокол Secure Sockets Layer (SSL) или Transport Layer Security (TLS) используется, чтобы обеспечить защиту на уровне транспорта для безопасной связи между серверами, клиентами, агентами хранения IBM Spectrum Protect и компонентом Центр операций. Если вы пересылаете данные между сервером, клиентом и агентом хранения, для шифрования данных используется SSL или TLS.



Ограничение: Не используйте протоколы SSL и TLS для связи с экземпляром базы данных IBM DB2, который используется сервером IBM Spectrum Protect.

У каждого сервера или агента хранения есть уникальный секретный ключ и уникальный подписанный сертификат, который используется, чтобы разрешить соединения SSL. Если вы используете самоподписанные сертификаты, самоподписанный сертификат для каждого сервера или агента хранения автоматически распределяется по всем клиентам, агентам хранения и серверам, которые используют TLS для связи с ними. Если вы используете сертификаты, подписанные центром сертификации (certificate authority, CA), каждый сервер и агент хранения IBM Spectrum Protect должны отправлять уникальный сертификат сервера на подпись в центр сертификации. CA возвращает подписанный сертификат сервера, который нужно добавить в базу данных ключей сервера вместе с корневым сертификатом CA и всеми промежуточными сертификатами CA. Сертификат сервера, подписанный CA, не нужно распределять по клиентам.

Если вы используете сертификаты, подписанные CA, все клиенты, у агентов хранения и серверов, использующих TLS для взаимодействий с сервером или агентом хранения, должны быть корневой сертификат и промежуточные сертификаты CA, установленные в соответствующей базе данных ключей. Корневой сертификат и промежуточные сертификаты CA используются для проверки сертификата сервера, подписанного CA. Сертификаты проверяются клиентом или сервером SSL, который затребовал или инициировал связь по SSL.

Сервер IBM Spectrum Protect принимает подписанные CA сертификаты, которые используют метод шифрования SHA-256 или более ранний метод SHA (Secure Hash Algorithm). Сертификаты SHA-256 разработаны, чтобы улучшить защиту и обеспечить соответствие требованиям National Institute of Standards and Technology (NIST). Поэтому предпочтительным методом является использование сертификатов SHA-256 для связи между сервером и компонентом Центр операций.

Если при обновлении до V8.1.4 или новее у сервера есть сертификат с подписью MD5 и меткой "TSM Server SelfSigned Key", заданный как сертификат по умолчанию, сертификат по умолчанию будет автоматически обновлен, так чтобы использовался сертификат с подписью SHA. В выпусках до V7.1.8 сертификатом по умолчанию был сертификат "TSM Server SelfSigned Key" с подписью MD5, который не поддерживал протокол TLS 1.2, необходимый по умолчанию для клиентов V8.1.2 или новее и центра операций. Начиная с V8.1.4, серверы, которые используют сертификат с подписью MD5, как сертификат по умолчанию, автоматически обновляются для использования сертификата по умолчанию с

подписью SHA и меткой "TSM Server SelfSigned SHA Key". Копия сертификата хранится в файле cert256.arm, находящемся в каталоге экземпляра сервера.

При связи сервер IBM Spectrum Protect, клиент или агент хранения могут служить клиентом SSL. Клиент SSL - это компонент, инициирующий связь и проверяющий сертификат для сервера SSL. Например, если клиент IBM Spectrum Protect инициирует связь по SSL с сервером IBM Spectrum Protect, данный клиент IBM Spectrum Protect - это клиент SSL, а сервер - это сервер SSL.

В разделе Табл. 1 перечислены компоненты, которые могут быть клиентом SSL или сервером SSL.

Табл. 1. Клиенты и серверы SSL в среде IBM Spectrum Protect

Клиент SSL	**Сервер SSL**	**Сценарий**
Клиент	Сервер	Клиент IBM Spectrum Protect инициирует требование связи с сервером IBM Spectrum Protect. Этот клиент проверяет сертификат. Сервер предоставляет сертификат.
Сервер (такой как сервер источника)	Сервер (такой как сервер назначения)	Сервер источника IBM Spectrum Protect инициирует требование связи с сервером назначения IBM Spectrum Protect. Сервер источника действует как клиент SSL и проверяет сертификат, предоставляемый сервером назначения. Это общий тип связи при обработке репликаций.
Клиент через агент хранения	Сервер	Клиент проверяет каждый сертификат, когда отдельно инициирует связь SSL с сервером IBM Spectrum Protect и агентом хранения. Когда агент хранения связывается с сервером с использованием протокола SSL, этот агент хранения действует как клиент SSL и проверяет сертификат, предоставляемый сервером. Агент хранения может одновременно быть и клиентом SSL, и провайдером SSL. Клиент должен использовать для взаимодействий с сервером и агентом хранения тот же протокол связи (SSL или TCP/IP).
Сервер	Сервер LDAP	Сервер IBM Spectrum Protect инициирует требование связи с сервером LDAP. Сервер IBM Spectrum Protect действует как клиент SSL и проверяет сертификат, предоставляемый сервером LDAP.
Центр операций	Сервер	Центр операций инициирует связь с сервером IBM Spectrum Protect. Центр операций действует как клиент SSL и проверяет сертификат, предоставляемый сервером IBM Spectrum Protect.
Отчеты	Сервер	Агент составления отчетов инициирует требование связи с сервером IBM Spectrum Protect. Возможность составления отчетов действует как клиент SSL и проверяет сертификат, предоставляемый сервером IBM Spectrum Protect.

Конфигурирование агентов хранения, серверов, клиентов и центра операций для соединения с сервером с использованием SSL

Сконфигурируйте Secure Sockets Layer (SSL) на сервере IBM Spectrum Protect, на клиенте резервного копирования и архивирования, на агенте хранения и в компоненте Центр операций, чтобы убедиться, что данные при взаимодействиях шифруются.

Можно использовать самоподписанный сертификат SSL или сертификат от стороннего центра сертификации (certificate authority, CA), чтобы проверять требование взаимодействий SSL между сервером, клиентом и агентом хранения. Каждый сервер IBM Spectrum Protect, клиент или агент хранения, на котором включается поддержка SSL, должен использовать доверенный самоподписанный сертификат или получить уникальный сертификат, подписанный сертификатором (CA).

Преимуществом сертификатов, подписанных CA, является то, что один сертификат, подписанный CA, можно использовать для всех серверов, и это позволит вам распространить один сертификат по клиентам. Если вы используете самоподписанный сертификат, сертификат создается автоматически для каждого сервера и агента хранения. Если вы используете корневой сертификат от сертификатора, его надо установить в каждой базе данных ключей для клиента, сервера и агента хранения, инициирующего соединение SSL. Сертификат проверяется клиентом или сервером SSL, который затребовал или инициировал связь по SSL.

Ограничение: Некоторые CA используют сертификаты в формате, который не распознается продуктом IBM Spectrum Protect. Возможно, вам придется обратиться к своему сертификатору, чтобы преобразовать сертификат в формат, который можно использовать вместе с IBM Spectrum Protect.

- Конфигурирование сервера для приема соединений SSL
  Прежде чем включать связь SSL с сервера с клиентом, агентом хранения или другим сервером, сконфигурируйте сервер для приема соединений SSL.
- Конфигурирование агента хранения для использования SSL
  Чтобы убедиться, что данные шифруются для взаимодействий между агентом хранения и сервером и агентом хранения и клиентом, сконфигурируйте агенты хранения для взаимодействий с использованием протокола SSL.
- Конфигурирование клиента для соединения с агентом хранения при помощи SSL
  Чтобы защитить данные, передаваемые между клиентом и агентом хранения, сконфигурируйте клиент для соединения с агентом хранения с использованием протокола SSL.

Конфигурирование сервера для приема соединений SSL

Прежде чем включать связь SSL с сервера с клиентом, агентом хранения или другим сервером, сконфигурируйте сервер для приема соединений SSL.

Об этой задаче

Используйте эту процедуру для конфигурирования вручную.

Процедура

1. Укажите порт, на котором сервер ожидает связи с клиентами с включенной поддержкой SSL, или примите номер порта по умолчанию. (Необязательно) Обновите файл dsmserv.opt в каталоге экземпляра сервера, задав опцию TCPPORT и/или TCPADMINPORT. Опции SSLTCPPORT и SSLTCPADMINPORT можрно использовать только для соединений SSL.
2. Создайте базу данных ключей сервера, запустив для этого сервер. Файл базы данных ключей сервера, cert.kdb сохраняется в каталоге экземпляра сервера, и метка сертификата по умолчанию автоматически задается как "TSM Server SelfSigned SHA Key". Сертификат экспортируется в файл cert256.arm.
3. Если вы используете самоподписанный сертификат по умолчанию, при соединении с сервером с использованием TLS вам потребуется файл самоподписанного сертификата по умолчанию (cert256.arm). После использования файла cert256.arm для импорта самоподписанного сертификата в базу данных ключей файл перестает быть нужен.
4. Если вы используете сертификат, подписанный CA, каждый сервер IBM Spectrum Protect должен отправить уникальный сертификат сервера на подпись в центр сертификации. Сертификатор возвращает подписанный сертификат сервера. Чтобы сконфигурировать сертификаты сертификатора, выполните для каждого сервера IBM Spectrum Protect:
   a. Импортируйте корневой сертификат CA для каждого сервера IBM Spectrum Protect, для которого будет включена поддержка SSL. Войдите в систему сервера IBM Spectrum Protect, используя ID пользователя экземпляра, и введите в каталоге экземпляра следующий пример команды:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -label "CA cert" -file ca.crt
      ```

   b. Импортируйте один или несколько промежуточных сертификатов CA, введя следующий пример команды для каждого промежуточного сертификата:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -label "Промежуточный сертификат CA" -
      file intca.crt
      ```

   c. Корневой сертификат и промежуточные сертификаты CA (ca.crt и intca.crt) используются для проверки сертификата сервера, подписанного CA. Корневой сертификат и промежуточные сертификаты CA нужно установить в базе данных ключей всех клиентов, агентов хранения и серверов, использующих TLS для взаимодействия с сервером.
   d. Создайте на сервере требование сертификата, чтобы CA подписал его, используя команду, аналогичную следующему примеру:

      ```
      gsk8capicmd_64 -certreq -create -db cert.kdb -stashed -label "CA cert"
      -sigalg sha256 -size 2048 -ku "digitalSignature,keyEncipherment,keyAgreement "
      -eku "clientAuth,serverAuth" -dn "CN=tucson.example.com,OU=Spectrum Protect,O=IBM"
      -san_dnsname tucson.example.com -san_ipaddr 9.11.0.0 -file cert_request.csr
      ```

e. Чтобы получить подписанный сертификат и сделать его сертификатом по умолчанию при взаимодействии с клиентами, введите следующий пример команды:

```
gsk8capicmd_64 -cert -receive -db cert.kdb -stashed -file cert_signed.crt
-default_cert yes
```

Сертификат сервера, подписанный CA, не нужно распределять по клиентам.

5. Если вы внесли изменения, перезапустите сервер.

Дальнейшие действия

Включите связь SSL с этим сервером с клиента, агента хранения или другого сервера. Чтобы выполнить следующие задачи, у вас должен быть сертификат сервера и номер порта, заданный для сервера.

1. Чтобы включить связь SSL с клиента с данным сервером, смотрите раздел Конфигурирование связи клиента/сервера IBM Spectrum Protect с Secure Sockets Layer.
2. Чтобы включить связь SSL с другого сервера с данным сервером, смотрите раздел Конфигурирование сервера для соединения с другим сервером при помощи SSL.
3. Чтобы включить связь SSL с агента хранения с данным сервером, смотрите раздел Конфигурирование агента хранения для использования SSL.
4. Чтобы включить связь SSL из центра операций с данным сервером, смотрите раздел Конфигурирование центра операций для соединения с хаб-сервером с использованием SSL.
5. Чтобы включить связь SSL из графического интерфейса Data Protection for VMware vSphere с данным сервером, смотрите раздел Конфигурирование графического интерфейса Data Protection for VMware для взаимодействий с сервером с использованием SSL.

- Конфигурирование клиентов для взаимодействий с сервером с использованием SSL
  Чтобы убедиться, что данные шифруются при взаимодействиях клиента с сервером, сконфигурируйте клиенты для взаимодействий с сервером с использованием протокола SSL.
- Конфигурирование сервера для соединения с другим сервером при помощи SSL
  Чтобы убедиться, что данные шифруются для взаимодействий сервера с сервером, сконфигурируйте серверы для взаимодействий с серверами с использованием протокола SSL.
- Конфигурирование центра операций для соединения с хаб-сервером с использованием SSL
  Чтобы убедиться, что данные шифруются для взаимодействий между центром операций и хаб-сервером, сконфигурируйте центр операций для взаимодействий с хаб-серверов с использованием протокола SSL.
- Конфигурирование графического интерфейса Data Protection for VMware для взаимодействий с сервером с использованием SSL
  Чтобы убедиться, что данные шифруются при взаимодействии с сервером IBM Spectrum Protect, сконфигурируйте графический пользовательский интерфейс Data Protection for VMware vSphere для взаимодействий с серверов с использованием протокола SSL.

Ссылки, связанные с данной:
TCPPORT
TCPADMINPORT
QUERY SESSION (запрос информации о клиентских сеансах)

Конфигурирование клиентов для взаимодействий с сервером с использованием SSL

Чтобы убедиться, что данные шифруются при взаимодействиях клиента с сервером, сконфигурируйте клиенты для взаимодействий с сервером с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат сервера и номер порта, используемый сервером. Дополнительные сведения смотрите в разделе Конфигурирование сервера для приема соединений SSL.

Процедура

Чтобы включить связь SSL между сервером и клиентами, смотрите раздел Конфигурирование связи клиента/сервера IBM Spectrum Protect с Secure Sockets Layer.

Конфигурирование сервера для соединения с другим сервером при помощи SSL

Чтобы убедиться, что данные шифруются для взаимодействий сервера с сервером, сконфигурируйте серверы для взаимодействий с серверами с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат и номер порта для сервера, с которым вы соединяетесь. Дополнительные сведения смотрите в разделе Конфигурирование сервера для приема соединений SSL.

Об этой задаче

Советы:

- Если оба сервера используют программу IBM Spectrum Protect V8.1.2 или новее, SSL конфигурируется автоматически. Конфигурирование вручную рекомендуется, но не требуется. Если какой-либо сервер использует ПО IBM Spectrum Protect ранее V8.1.2 или ПО Tivoli Storage Manager ранее V7.1.8, то надо вручную сконфигурировать SSL.
- В V8.1.2 надо вручную сконфигурировать агенты хранения на использование SSL. В V8.1.3 агенты хранения автоматически сконфигурированы для использования SSL.

В этой процедуре в качестве примеров используются следующие адреса серверов:

- ServerA (сервер, с которым вы соединяетесь) находится по адресу `bfa.tucson.example.com`
- Сервер ServerB находится по адресу `bfb.tucson.example.com`

Процедура

1. Создайте базу данных ключей сервера, запустив для этого сервер. Файл базы данных ключей сервера, cert.kdb, хранится в каталоге экземпляра сервера.
2. Для каждого сервера импортируйте файл самоподписанного сертификата (cert256.arm) другого сервера или сертификата CA. Чтобы импортировать самоподписанный сертификат, введите следующую команду:

   ```
   gsk8capicmd_64 -cert -add -label ip_адрес_сервера -db cert.kdb -stashed
   -file cert256.arm
   ```

   Совет: Используйте IP-адрес сервера в качестве имени метки.
3. Можно просмотреть сертификаты в базе данных ключей на каждом из серверов при помощи следующей команды:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

4. Перезапустите серверы.
5. Введите команду DEFINE SERVER.
   a. Для ServerA введите следующую команду:

      ```
      DEFINE SERVER BFB hla=bfb.tucson.example.com lla=1542
      serverpa=passwordforbfb SSL=YES
      ```

   b. Для ServerB введите следующую команду:

      ```
      DEFINE SERVER BFA hla=bfa.tucson.example.com lla=1542
      serverpa=passwordforbfa SSL=YES
      ```

Ссылки, связанные с данной:
QUERY SESSION (запрос информации о клиентских сеансах)
TCPPORT
TCPADMINPORT
DEFINE SERVER (Задать сервер для обмена данными между серверами)

Конфигурирование центра операций для соединения с хаб-сервером с использованием SSL

Чтобы убедиться, что данные шифруются для взаимодействий между центром операций и хаб-сервером, сконфигурируйте центр операций для взаимодействий с хаб-серверов с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат хаб-сервера и номер порта, используемый сервером. Дополнительные сведения смотрите в разделе Конфигурирование сервера для приема соединений SSL.

Процедура

Чтобы сконфигурировать связь SSL с центром операций, смотрите раздел Защита связи между компонентом Центр операций и хаб-сервером.

Конфигурирование графического интерфейса Data Protection for VMware для взаимодействий с сервером с использованием SSL

Чтобы убедиться, что данные шифруются при взаимодействии с сервером IBM Spectrum Protect, сконфигурируйте графический пользовательский интерфейс Data Protection for VMware vSphere для взаимодействий с серверов с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат сервера и номер порта, используемый сервером. Дополнительные сведения смотрите в разделе Конфигурирование сервера для приема соединений SSL.

Процедура

Чтобы включить связь SSL между сервером и Data Protection for VMware vSphere GUI, смотрите раздел Обеспечение защищенного обмена информацией с сервером IBM Spectrum Protect.

Конфигурирование агента хранения для использования SSL

Чтобы убедиться, что данные шифруются для взаимодействий между агентом хранения и сервером и агентом хранения и клиентом, сконфигурируйте агенты хранения для взаимодействий с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат сервера и номер порта, используемый сервером. Дополнительные сведения смотрите в разделе Конфигурирование сервера для приема соединений SSL.

Процедура

1. Инициализируйте агент хранения и добавьте информацию о связи в файл конфигурации устройства и в файл опций агента хранения dsmsta.opt, введя команду DSMSTA SETSTORAGESERVER. Чтобы создать файл базы данных ключей в файле dsmsta.opt, нужно задать параметр SSL=YES. Все пароли шифруются в dsmsta.opt.

   ```
   dsmsta setstorageserver myname=имя_агента_хранения mypa=пароль_sta
   myhla=ip_адрес servername=имя_сервера serverpa=пароль_сервера
   hla=ip_адрес lla=порт_ssl ssl=yes
   ```

2. Создайте сертификат базы данных ключей и сертификаты по умолчанию, запустив агент хранения.
3. Импортируйте для агента хранения и сервера файл cert256.arm или файлы сертификатов CA други агентов хранения и серверов:

   ```
   gsk8capicmd_64 -cert -add -label ip_адрес -db cert.kdb -stashed
   -file cert256.arm
   ```

   Совет: Используйте IP-адрес в качестве имени метки.
4. Можно просмотреть сертификаты в базе данных ключей при помощи следующей команды:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

5. Перезапустите агент хранения и сервер.
6. Установите связь между сервером и агентом хранения, введя следующую команду:

```
define server sta hla=ip_адрес lla=порт serverpa=пароль ssl=yes
```

Ссылки, связанные с данной:
QUERY SESSION (запрос информации о клиентских сеансах)
TCPPORT
TCPADMINPORT
DEFINE SERVER (Задать сервер для обмена данными между серверами)

Конфигурирование клиента для соединения с агентом хранения при помощи SSL

Чтобы защитить данные, передаваемые между клиентом и агентом хранения, сконфигурируйте клиент для соединения с агентом хранения с использованием протокола SSL.

Прежде чем начать

У вас должен быть сертификат и номер порта для агента хранения.

Об этой задаче

После конфигурирования агента хранения для принятия соединений SSL, сконфигурируйте клиенты для соединения с агентом хранения при помощи SSL.

Процедура

Чтобы включить связь SSL между клиентами и агентом хранения, смотрите раздел Конфигурирование связи клиента/сервера IBM Spectrum Protect с Secure Sockets Layer.
Ссылки, связанные с данной:
TCPPORT
TCPADMINPORT

Аутентификация пользователей IBM Spectrum Protect с использованием сервера LDAP

В системе IBM Spectrum Protect пользователи должны аутентифицироваться на сервере, вводя ID пользователя и пароль. Если ваша организация использует для управления ID пользователей сервер Lightweight Directory Access Protocol (LDAP), можно с помощью сервера LDAP аутентифицировать ID пользователей IBM Spectrum Protect.

Можно использовать один из следующих методов для аутентификации пользователей на сервере LDAP:

Метод, который является предпочтительным для IBM® Tivoli Storage Manager версии 7.1.7 и новее и для серверов IBM Spectrum Protect версии 8.1 и новее.

Чтобы использовать этот метод, который иногда называют *интегрированным режимом*, ID пользователей должны быть зарегистрированы в базе данных Active Directory на сервере LDAP. Затем этих же пользователей надо зарегистрировать на сервере IBM Spectrum Protect. Когда зарегистрированный ID пользователя обращается к серверу IBM Spectrum Protect, его параметры аутентификации сравниваются с данными базы данных Active Directory.
Чтобы использовать этот метод, выполните инструкции из раздела Аутентификация пользователей с использованием базы данных Active Directory.

Метод, используемый для серверов более ранних версий, чем V7.1.7, пользователями IBM Security Directory Server

Для использования этого метода ID пользователей должны быть зарегистрированы в базе данных Active Directory на сервере LDAP. Другой вариант - ID пользователей можно зарегистрировать в базе данных IBM Security Directory Server (ранее IBM Tivoli Directory Server) на сервере LDAP. С этим методом нельзя использовать стандартные учетные записи пользователей, зарегистрированных на сервере LDAP. Необходимо создать отдельные учетные записи, связанные с конкретной организационной единицей. Чтобы использовать этот метод, следуйте инструкциям в разделе Управление паролями и процедурами входа в систему (V7.1.1).

- Аутентификация пользователей с использованием базы данных Active Directory
  Вы можете аутентифицировать пользователей IBM Spectrum Protect с помощью базы данных Active Directory на сервере Lightweight Directory Access Protocol (LDAP). С этим методом используются стандартные учетные записи пользователей, зарегистрированных на сервере LDAP. Для аутентификации на сервере IBM Spectrum Protect и на сервере LDAP может использоваться один и тот же ID пользователя.

Репликация данных клиента на другой сервер

Репликация данных клиента с исходного сервера на другой сервер помогает убедиться, что в случае повреждения исходного сервера для восстановления будет доступна резервная копия данных клиента. При репликации производится инкрементное копирование данных с исходного сервера на сервер назначения, чтобы обеспечить возможность передачи управления в случае отказа и возврата управления.

Об этой задаче

Если произойдет авария и сервер источника временно окажется недоступен, то клиентские узлы смогут восстановить свои данные с сервера назначения. Если сервер источника восстановить невозможно, то вы можете изменить конфигурацию клиентского узла для хранения данных на сервере назначения. В случае сбоя исходный сервер сможет автоматически передать управление серверу назначения для восстановления данных.
Ограничение: Сервер может реплицировать данные только на один целевой сервер репликации.
Можно реплицировать данные, хранящиеся в пуле хранения любого типа. Тип пула хранения может быть разным на исходном сервере репликации и на целевом сервере репликации. Вы можете управлять репликацией на основе типа данных клиентского узла:

- Данные активных и неактивных резервных копий или только данные активных резервных копий
- Архивные данные
- Данные, перенесенные на сервер источника клиентами IBM Spectrum Protect for Space Management

При репликации данных в пулах хранения каталогов-контейнеров используйте защиту пулов, чтобы повысить эффективность процесса репликации и включить исправление данных. При использовании компонента Центр операций для настройки пулов хранения расписания по защите определяются автоматически, так чтобы они согласовывались с расписанием репликации.

Процедура

1. Проверьте, совместимы ли серверы и есть ли системные ресурсы для успешного использования репликации.

   Требуются более высокие объемы памяти и большее число ядер процессора. Размеры базы данных и ее журналов должны быть подобраны, так чтобы гарантировать возможность успешного завершения транзакции. Требуется выделенная сеть с достаточной шириной полосы пропускания, чтобы обработать объем данных, которые вы собираетесь реплицировать.

   a. Убедитесь, что исходный сервер и сервер назначения совместимы для репликации. Смотрите раздел Совместимость репликации.
   b. Убедитесь, что у сервера есть соответствующие ресурсы для хорошей производительности. Дополнительные сведения смотрите в разделе Контрольный список для репликации узла.
2. Разрешитье репликацию. Смотрите раздел Как включить репликацию узлов.
3. Запланируйте репликацию для исходного сервера. Информацию о том, как интегрировать это расписание с расписаниями обычного обслуживания сервера, смотрите в разделе Как задать расписания для операций по обслуживанию серверов.
4. Запланируйте защиту пулов хранения для всех пулов хранения каталогов-контейнеров на исходном сервере. Смотрите раздел Защита данных в пулах хранения каталогов-контейнеров.
5. Отслеживайте репликацию, используя Центр операций. Дополнительную информацию смотрите в разделе Контрольный список ежедневного мониторинга.

- Совместимость репликации
  Прежде чем настраивать операции репликации IBM Spectrum Protect, вы должны убедиться, что исходный сервер репликации и сервер репликации назначения совместимы для репликации.
- Как включить репликацию узлов
  Вы можете включить репликацию узлов, чтобы защитить данные.
- Защита данных в пулах хранения каталогов-контейнеров
  Защитите данные в пулах хранения каталогов-контейнеров, чтобы сократить время репликации узла и включить

исправление данных в пулах хранения каталогов-контейнеров.

- Изменение параметров репликации
  Измените параметры репликации в Центр операций. Измените такие параметры, как число сеансов репликации, правила репликации, данные, которые вы хотите реплицировать, расписание репликации и рабочую нагрузку репликации.
- Как задать разные политики сохранения для исходного сервера и целевого сервера
  Вы можете задать политики на сервере назначения репликации, которые будут управлять реплицированными данными узлов-клиентов не так, как на исходном сервере. Например, можно обслуживать разное число версий файлов на исходном сервере и на сервере назначения.

Совместимость репликации

Прежде чем настраивать операции репликации IBM Spectrum Protect, вы должны убедиться, что исходный сервер репликации и сервер репликации назначения совместимы для репликации.

Табл. 1. Совместимость репликации для разных версий серверов

Версия сервера репликации источника	**Совместимые версии для сервера репликации назначения**
V7.1	Версия 7.1 или более поздняя
Версия 7.1.1	Версия 7.1 или более поздняя
V7.1.3	V7.1.3 или новее
V7.1.4	V7.1.3 или новее
V7.1.5	V7.1.3 или новее
V7.1.6	V7.1.3 или новее
Версия 7.1.7	V7.1.3 или новее
V7.1.8	V7.1.3 или новее
V8.1	V7.1.3 или новее
V8.1.1	V7.1.3 или новее
V8.1.2	V7.1.3 или новее
V8.1.3	V7.1.3 или новее
V8.1.4	V7.1.3 или новее
V8.1.5	V7.1.3 или новее

Как включить репликацию узлов

Вы можете включить репликацию узлов, чтобы защитить данные.

Прежде чем начать

Убедитесь, что исходный сервер и сервер назначения совместимы для репликации.

Об этой задаче

Реплицируйте клиентский узел, чтобы реплицировать все данные клиента, включая метаданные. По умолчанию, когда вы впервые запускаете сервер, репликация узлов будет отключена.
Советы:

- Чтобы сократить время обработки репликации, защитите пул хранения до репликации клиентских узлов. При запуске репликации узла экстенты данных, которые уже были реплицированы за счет защиты пула хранения, будут пропущены.
- Для репликации требуются увеличенные объемы памяти достаточная полоса пропускания для выполнения обработки. Задайте такие размеры базы данных и ее журналов, чтобы транзакции могли выполняться.

Процедура

Чтобы включить репликацию узлов, выполните в компоненте Центр операций следующие шаги:

a. Щелкните на странице Серверы по Сведения.
b. На странице Сведения щелкните по Свойства.
c. В разделе Репликация выберите Включена в поле Исходящая репликация.
d. Щелкните по Сохранить.

Дальнейшие действия

Выполните следующие действия:

1. Чтобы узнать, успешно ли выполнена репликация, смотрите раздел Контрольный список ежедневного мониторинга.
2. Операционные системы LinuxЕсли сервер IBM Spectrum Protect реплицирует узлы на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Выполните инструкции в разделе Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде.

Защита данных в пулах хранения каталогов-контейнеров

Защитите данные в пулах хранения каталогов-контейнеров, чтобы сократить время репликации узла и включить исправление данных в пулах хранения каталогов-контейнеров.

Прежде чем начать

Убедитесь, что на целевом сервере репликации существует хотя бы один пул хранения каталогов-контейнеров. Включив репликацию в компоненте Центр операций, можно запланировать защиту пула хранения. Чтобы сконфигурировать репликацию и включить защиту пула хранения, выполните следующие шаги:

1. В строке меню компонента Центр операций установите указатель мыши на Хранение и щелкните по Репликация.
2. На странице Репликация щелкните по Пара серверов.
3. Выполните шаги в мастере Добавить пару серверов.

Об этой задаче

При защите пулов хранения каталогов-контейнеров производится резервное копирование экстентов данных в другой пул хранения, и это позволяет повысить производительность при репликации узлов. При запуске репликации узла экстенты данных, резервное копирование которых уже было произведено за счет защиты пула хранения, будут пропущены, что сокращает время обработки репликации. Можно задать расписание защиты пулов хранения несколько раз в день, чтобы успевать за изменениями данных.

Защищая пул хранения, вы не используете ресурсы, которые реплицируют существующие данные и метаданные, что позволяет повысить производительность сервера. Если вы хотите защищать только пул хранения и создавать только его резервную копию, нужно использовать пулы хранения каталогов-контейнеров.

Альтернативная стратегия защиты: В качестве альтернативы использованию репликации можно защитить данные в пулах хранения каталогов-контейнеров, скопировав их в пулы хранения контейнеров-копий. Данные в пулах хранения контейнеров-копий хранятся на ленточных томах. Ленточные копии, хранящиеся автономно, дают дополнительную возможность защиты путем аварийного восстановления в реплицированной среде.

Процедура

1. Либо, чтобы включить защиту пула хранения, можно использовать команду PROTECT STGPOOL с исходного сервера, чтобы произвести резервное копирование экстентов данных в пуле хранения каталога-контейнера. Например, чтобы защитить пул хранения каталога-контейнера с именем POOL1, введите следующую команду:

   ```
   protect stgpool pool1
   ```

   В процессе операции по выполнению команды PROTECT STGPOOL исправляются поврежденные экстенты в пуле хранения назначения. Чтобы исправить экстенты, они должны уже быть отмечены на сервере назначения как

поврежденные. Например, команда AUDIT CONTAINER может выявить повреждение в пуле хранения назначения до ввода команды PROTECT STGPOOL.

2. Необязательно: Если поврежденные экстенты были исправлены в пуле хранения назначения и вы защищаете несколько исходных пулов хранения в одном пуле хранения назначения, выполните описанные ниже шаги, чтобы обеспечить полное исправление:
    a. Введите команду PROTECT STGPOOL для всех исходных пулов хранения, чтобы максимально исправить повреждение.
    b. Снова введите команду PROTECT STGPOOL для всех исходных пулов хранения. Для второй операции используйте параметр FORCERECONCILE=YES. Этот шаг гарантирует, что все исправления из других исходных пулов будут правильно распознаны для всех исходных пулов хранения.

Результаты

Если пул хранения каталога-контейнера защищен, вы сможете исправить пул хранения в случае его повреждения, используя команду REPAIR STGPOOL.
Ограничение: Если вы реплицируете клиентские узлы, но не защищаете пул хранения каталога-контейнера, вы не сможете исправить пул хранения.

Дальнейшие действия

Выполните следующие действия:

1. Чтобы увидеть состояние рабочей нагрузки по репликации, выполните инструкции в разделе Контрольный список ежедневного мониторинга.
2. Операционные системы LinuxЕсли сервер IBM Spectrum Protect реплицирует узлы на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Выполните инструкции в разделе Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде.

Задачи, связанные с данной:
Копирование пулов хранения каталогов-контейнеров на ленту
Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
PROTECT STGPOOL (Защитить данные пула хранения)

Изменение параметров репликации

Измените параметры репликации в Центр операций. Измените такие параметры, как число сеансов репликации, правила репликации, данные, которые вы хотите реплицировать, расписание репликации и рабочую нагрузку репликации.

Об этой задаче

Вам может потребоваться настроить параметры репликации в следующих сценариях:

- Изменения приоритетов данных
- Изменения правил репликации
- Необходимость сделать целевым сервером другой сервер
- Запланированные процессы, отрицательно влияющие на производительность сервера

Процедура

Используйте компонент Центр операций, чтобы изменить параметры репликации.

Задача	Процедура

Задача	Процедура
Измените правило репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация выберите правило репликации, которое вы хотите применить: Правило архивирования по умолчанию, Правило резервного копирования по умолчанию или Правило управления пространством по умолчанию. d. Щелкните по Сохранить.
Укажите, в течение какого времени сохраняются записи репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация введите срок в днях, в течение которого должны храниться записи репликации, в поле Сохранять хронологию репликации. Либо выберите переключатель Не сохранять, если вам не нужны записи репликации. d. Щелкните по Сохранить.
Задайте целевой сервер репликации.	a. Щелкните на странице Серверы по Сведения. b. На странице Сведения щелкните по Свойства. c. В разделе Репликация задайте целевой сервер. d. Щелкните по Сохранить.
Отмените процесс репликации.	a. Щелкните на странице Серверы по Активные задачи. b. Выберите процесс или сеанс, который вы хотите отменить. c. Нажмите кнопку Отмена.

Как задать разные политики сохранения для исходного сервера и целевого сервера

Вы можете задать политики на сервере назначения репликации, которые будут управлять реплицированными данными узлов-клиентов не так, как на исходном сервере. Например, можно обслуживать разное число версий файлов на исходном сервере и на сервере назначения.

Процедура

1. На исходном сервере репликации проверьте конфигурацию репликации и убедитесь, что исходный сервер репликации может взаимодействовать с целевым сервером репликации; для этого введите команду VALIDATE REPLPOLICY. Например, проверьте конфигурацию, используя имя одного из реплицируемых клиентских узлов:

   ```
   validate replication node1 verifyconnection=yes
   ```

2. На исходном сервере репликации введите команду VALIDATE REPLPOLICY, чтобы проверить различия в политиках на серверах репликации источника и назначения. Например, чтобы увидеть разницу в политиках на исходном сервере и на сервере назначения, CVT_SRV2, введите на исходном сервере следующую команду:

   ```
   validate replpolicy cvt_srv2
   ```

3. Обновите политики на сервере назначения, если это потребуется.
   Совет: Можно использовать компонент Центр операций, чтобы изменить политики на сервере назначения. Следуйте инструкциям в Изменение политик.
   Например, чтобы хранить неактивные версии файлов на сервере назначения в течение более короткого времени, чем на исходном сервере, уменьшите значение параметра Резервные копии в классах управления, применимых к реплицированным данным клиента.
4. Включите политики сервера репликации назначения, так чтобы он использовал свои политики для управления реплицированными данными клиентского узла; для этого введите на исходном сервере команду SET DISSIMILARPOLICIES. Например, чтобы включить политики на сервере репликации назначения CVT_SRV2, введите на исходном сервере следующую команду:

   ```
   set dissimilarpolicies cvt_srv2 on
   ```

В следующий раз, когда запустится процесс репликации, политики на сервере репликации назначения будут использоваться для управления реплицированными данными клиентского узла.
Совет: Если вы сконфигурируете репликацию, используя Центр операций, а политики на исходном сервере репликации и на сервере репликации назначения не совпадают, будет использоваться политика, заданная для исходного сервера репликации. Если вы включите политику на сервере репликации назначения, используя команду SET DISSIMILARPOLICIES, будет использоваться политика, заданная для сервера репликации назначения. Если на сервере репликации назначения нет политики, используемой узлом на исходном сервере репликации, используется политика STANDARD.

Ссылки, связанные с данной:
EXPORT POLICY (экспорт сведений политики)
SET DISSIMILARPOLICIES (включить политики на сервере репликации назначения, чтобы управлять реплицированными данными)
VALIDATE REPLICATION (Проверить репликацию для клиентского узла)
VALIDATE REPLPOLICY (Проверить политики на сервере репликации назначения)
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Конфигурирование кластерных сред

Сервер IBM Spectrum Protect можно сконфигурировать для кластеризации в системах AIX, Linux или Windows.

Кластерную среду можно использовать для следующих операционных систем:

- IBM® PowerHA SystemMirror for AIX
- IBM Tivoli System Automation for Multiplatforms for AIX and Linux
- Microsoft Failover Cluster for Windows

Можно использовать другие кластерные продукты с IBM Spectrum Protect, однако документация для них недоступна и поддержка ограничена. Последнюю информацию о поддержке для кластеризованных сред смотрите в разделе http://www.ibm.com/support/docview.wss?uid=swg21609772.

Перед использованием какого-то нового кластерного продукта убедитесь, что DB2 поддерживает необходимые файловые системы. Дополнительную информацию об используемом уровне DB2 смотрите на сайте Информация о DB2; найдите рекомендованные файловые системы.

- Обзор кластерных сред
  Кластеры состоят из многих компонентов: серверов IBM Spectrum Protect, аппаратных компонентов и программного обеспечения. Кластеризацию можно использовать для объединения двух или более серверов или узлов при помощи системы дисков совместного использования.
- Операционные системы AIXКонфигурирование среды AIX для кластеризации
  Сервер IBM Spectrum Protect можно сконфигурировать для кластерных сред AIX, используя IBM PowerHA SystemMirror для AIX или IBM Tivoli System Automation for Multiplatforms.
- Операционные системы LinuxКонфигурирование среды Linux для кластеризации
  Можно сконфигурировать сервер Linux IBM Spectrum Protect в кластерной среде посредством IBM Tivoli System Automation for Multiplatforms версии 4.1.
- Операционные системы WindowsКонфигурирование кластерной среды Windows
  Вы можете сконфигурировать сервер IBM Spectrum Protect для Windows в среде Microsoft Failover Cluster. Кластерные среды Windows состоят из следующих компонентов: серверов IBM Spectrum Protect, аппаратных компонентов и программного обеспечения. Когда эти компоненты соединены с одной дисковой системой, время простоя минимизируется.

Информация, связанная с данной:
Обновление сервера в кластерной среде
Операционные системы AIX Операционные системы Linux Операционные системы Windows

Обзор кластерных сред

Кластеры состоят из многих компонентов: серверов IBM Spectrum Protect, аппаратных компонентов и программного обеспечения. Кластеризацию можно использовать для объединения двух или более серверов или узлов при помощи системы дисков совместного использования.

Эта конфигурация позволяет узлам совместно использовать данные, что обеспечивает высокую доступность сервера и минимальное время простоя. Например:

- Можно сконфигурировать и отслеживать прикладные программы и аппаратные компоненты, внедренные в кластере, а также управлять ими.
- Вы можете, используя интерфейс управления кластером и IBM Spectrum Protect, задать организацию кластера и шаблон передачи управления при отказах. Сервер - это часть кластера, предоставляющего дополнительный уровень защиты и обеспечивающего отсутствие потерь транзакций при отказах сервера. Заданный вами порядок обработки отказов предотвратит сбои в будущем.
- Кластеризацию можно применить для процесса репликации узла. При этом доступность сервера будет выше, чем в случае репликации узла как его собственного процесса. Доступность сервера будет выше, так как в кластерной среде клиент менее вероятно передаст управление на другой сервер. Если данные реплицируются с нескольких исходных серверов репликации на один сервер репликации назначения, успех процесса существенно зависит от сервера назначения. В кластеризованной среде эта зависимость от сервера репликации назначения ослабляется.

Компоненты в серверном кластере называются *объектами кластера*. Объекты кластера связаны с набором свойств, у которых есть значения данных, описывающих идентичность и поведение объекта в кластере. К объектам кластера могут относится следующие компоненты:

- Узлы
- Хранение
- Службы и приложения
- Сети

Вы можете управлять кластерными объектами, изменяя их свойства; обычно это делается при помощи приложения для управления кластером.

- Узлы кластера
  Все узлы в кластере обладают сходными характеристиками, что позволяет им работать совместно друг с другом.

Операционные системы AIX

Конфигурирование среды AIX для кластеризации

Сервер IBM Spectrum Protect можно сконфигурировать для кластерных сред AIX, используя IBM® PowerHA SystemMirror для AIX или IBM Tivoli System Automation for Multiplatforms.

PowerHA SystemMirror для AIX и System Automation for Multiplatforms обнаруживают системные сбои и управляют передачей управления процессору восстановления с минимальной потерей времени для пользователей. Сервер IBM Spectrum Protect можно установить в кластере PowerHA или System Automation for Multiplatforms. После этого если на компьютере произойдет сбой, то сервер IBM Spectrum Protect может запуститься на другом компьютере в кластере.

Как в случае переключения после отказа, так и в случае восстановления кажется, что сервер IBM Spectrum Protect остановился и перезапустился. Для всех транзакций, которые выполнялись во время переключения или восстановления после отказа, выполняется откат, а все завершенные транзакции остаются выполненными. Клиенты IBM Spectrum Protect воспринимают переключение и восстановление как сбой связи и пытаются повторно установить соединение.

Подробности об этих опциях кластеризации смотрите в следующей информации.

- Сконфигурируйте IBM Spectrum Protect for AIX для использования IBM PowerHA SystemMirror for AIX в кластерной среде; для этого ознакомьтесь со следующими разделами.
- Сконфигурируйте IBM Spectrum Protect for AIX для использования System Automation for Multiplatforms в кластерной среде; для этого ознакомьтесь с информацией на веб-странице http://www.ibm.com/support/docview.wss?uid=swg27039780.
- Узнайте подробнее о Информация о PowerHA SystemMirror.

- Операционные системы AIXТребования к кластеру PowerHA
  IBM PowerHA SystemMirror for AIX обнаруживает системные сбои и управляет передачей управления процессору восстановления с минимальной потерей времени для пользователей.
- Операционные системы AIXПередача управления при отказе и возврат управления при использовании PowerHA
  Если в работе узла возникает сбой, сервер кластера передает группы, для которых хостом является данный узел, другим узлам кластера. Этот процесс передачи называется *обработкой отказа*. Обратный процесс, *восстановление после отказа*, выполняется, когда отказавший узел снова становится активным, и группы, переданные другим узлам, повторно передаются исходному узлу.

- Операционные системы AIXУстановка и конфигурирование PowerHA SystemMirror для AIX
  Сервер IBM Spectrum Protect можно сконфигурировать для кластерных сред AIX, используя IBM PowerHA SystemMirror для AIX.
- Операционные системы AIXУстановка сервера IBM Spectrum Protect на производственном узле для PowerHA
  Установите сервер IBM Spectrum Protect на производственном узле для PowerHA, чтобы можно было сконфигурировать его для кластеризации.
- Операционные системы AIXУстановка клиента IBM Spectrum Protect на производственном узле для PowerHA
  Нужно установить только набор файлов клиента резервного копирования и архивирования, содержащий файлы клиента резервного копирования и архивирования и клиента командной строки администрирования.
- Операционные системы AIXПроверка конфигурации сервера IBM Spectrum Protect для PowerHA
  Когда сервер IBM Spectrum Protect будет сконфигурирован для использования PowerHA, необходимо проверить его конфигурацию.
- Операционные системы AIXКак настроить резервный узел для PowerHA
  При использовании PowerHA, прежде чем настраивать резервный узел, убедитесь, что сервер IBM Spectrum Protect не работает на производственном узле.
- Операционные системы AIXКак задать устройства хранения со сменными носителями в AIX для PowerHA
  В операционной системе AIXнеобходимо определить устройства хранения со сменными носителями, которые используются IBM Spectrum Protect на производственных и резервных узлах. Менеджер библиотеки проверяет, находится ли картридж, содержщий устройство хранения съемного носителя, в правильном накопителе.
- Операционные системы AIXЗавершение конфигурирования менеджера кластера и IBM Spectrum Protect
  Измените конфигурацию менеджера кластера, чтобы задать сервер IBM Spectrum Protect как приложение и ресурс переключения после отказа резервного узла. Этим приложением владеет производственный узел.
- Операционные системы AIXУстранение неисправностей кластерной среды PowerHA
  Посмотрите в следующем списке информацию об общих проблемах диагностики и устранения неисправностей. В информации, приведенной для IBM PowerHA SystemMirror for AIX, представлены не все возможные сценарии.

Операционные системы AIX

Требования к кластеру PowerHA

IBM PowerHA SystemMirror for AIX обнаруживает системные сбои и управляет передачей управления процессору восстановления с минимальной потерей времени для пользователей.

При конфигурировании сервера IBM Spectrum Protect действуют следующие требования к аппаратному обеспечению:

- Аппаратная конфигурация, подходящая для PowerHA. Устройства хранения со сменными носителями для сервера IBM Spectrum Protect должны быть физически подсоединены по крайней мере к двум узлам кластера PowerHA на совместно используемой шине (включая SAN).
- Требуется достаточный объем совместно используемого дискового пространства для размещения базы данных, журналов восстановления, каталога экземпляра и дисковых пулов хранения IBM Spectrum Protect, которые будут использоваться. Чтобы узнать, какой объем пространства потребуется для базы данных и журнала восстановления и как обеспечить доступность базы данных и журнала восстановления, смотрите раздел Управление емкостью перечня.
- Сеть TCP/IP.

Совет: Если сервер IBM Spectrum Protect управляет устройствами хранения со сменными носителями, вы можете сконфигурировать два сервера IBM Spectrum Protect для работы на разных компьютерах в кластере PowerHA. Если на одном из компьютеров произойдет сбой, оба сервера смогут работать на другом компьютере. Чтобы сконфигурировать два сервера IBM Spectrum Protect для работы в разных системах в кластере PowerHA, используйте другую файловую систему, которая доступна для обоих серверов.
Операционные системы AIX

Передача управления при отказе и возврат управления при использовании PowerHA

Если в работе узла возникает сбой, сервер кластера передает группы, для которых хостом является данный узел, другим узлам кластера. Этот процесс передачи называется *обработкой отказа*. Обратный процесс, *восстановление после отказа*, выполняется, когда отказавший узел снова становится активным, и группы, переданные другим узлам, повторно передаются исходному узлу.

Терминами *производственный узел* и *резервный узел* обозначаются два узла PowerHA, на которых работает сервер IBM Spectrum Protect.

PowerHA управляет передачей адреса TCP/IP и монтированием совместно используемой файловой системы на резервном или на производственном узле в соответствии с ситуацией.

При выполнении *переключения после отказа* или *восстановления* для всех транзакций, которые обрабатывались в этот момент, выполняется откат. Клиентам IBM Spectrum Protect *переключение после отказа* или *восстановление* представляется как ошибка связи. Поэтому необходимо повторно установить соединение на основании значений опций клиентов COMMRESTARTDURATION и COMMRESTARTINTERVAL.

Обычно клиент резервного копирования и архивирования можно перезапустить от последней принятой транзакции. Если в момент обработки *переключения после отказа* запущено расписание клиента, то его работа может прерваться. Если вы можете повторно запустить операции клиента, то необходимо сделать это от начала обработки. Операции клиентов и агента выполняются, как в случае обычной остановки и перезапуска сервера, произошедшей во время сеанса их взаимодействия с сервером. Единственное отличие заключается в том, что сервер физически перезапускается на другом компьютере.

Если вы не хотите, чтобы *восстановление* выполнялось автоматически, то вы можете сконфигурировать ресурс как каскадную группу ресурсов без поддержки *восстановления*.

Информация, связанная с данной:
Информация о PowerHA SystemMirror

Установка и конфигурирование PowerHA SystemMirror для AIX

Сервер IBM Spectrum Protect можно сконфигурировать для кластерных сред AIX, используя IBM® PowerHA SystemMirror для AIX.

- Операционные системы AIXУстановка и конфигурирование кластера PowerHA
  Если не выполнить правильно установку и конфигурирование IBM PowerHA SystemMirror for AIX, можно столкнуться с ошибками обработки.
- Операционные системы AIXКонфигурирование сервера IBM Spectrum Protect на основном узле для PowerHA
  Можно сконфигурировать экземпляр сервера IBM Spectrum Protect на основном узле.
- Операционные системы AIXКонфигурирование сервера IBM Spectrum Protect на дополнительном узле для PowerHA с общим экземпляром DB2
  Если каталог экземпляра DB2 совместно используется узлами в кластере PowerHA, то создавать экземпляр DB2 на дополнительном узле не нужно. Не запускайте мастер dsmicfgx.
- Операционные системы AIXКонфигурирование сервера IBM Spectrum Protect на дополнительном узле для PowerHA с отдельным экземпляром DB2
  Нужно создать экземпляр DB2 на каждом дополнительном узле, если каталог экземпляра DB2 /home/tsminst1/sqllib не используется узлами совместно в кластере PowerHA.

Операционные системы AIX

Установка и конфигурирование кластера PowerHA

Если не выполнить правильно установку и конфигурирование IBM PowerHA SystemMirror for AIX, можно столкнуться с ошибками обработки.

Процедура

Чтобы установить и сконфигурировать кластер PowerHA, выполните следующие действия:

1. Задайте совместно используемые файловые и логические тома. Можно разместить файлы в отдельных файловых системах или на отдельных физических дисках, чтобы обеспечить целостность данных или необходимый уровень производительности. Не помещайте домашний каталог экземпляра пользователя на совместно используемый диск. Чтобы обеспечить максимальную доступность, сконфигурируйте зеркальное копирование логических томов (включая соответствующие файловые системы). В число файловых систем, которые нужно задать, входят каталог экземпляра сервера IBM Spectrum Protect, каталоги базы данных, каталоги журналов, все каталоги дисковых пулов хранения и каталоги пулов хранения, относящихся к типу устройств FILE.

2. Сконфигурируйте PowerHA, так чтобы производственный узел являлся владельцем групп совместно используемых томов, а резервный узел принимал на себя управления группами совместно используемых томов в случае отказа производственного узла.
3. Сконфигурируйте PowerHA, чтобы также осуществлялась передача управления для файловых систем.
4. Сконфигурируйте для сервера IBM Spectrum Protect IP-адрес службы. Этот IP-адрес службы должен отличаться ото всех IP-адресов хостов. С хоста на хост будет передаваться не фактический IP-адрес хоста, а IP-адрес службы.
5. Выполните передачу функций для совместно используемой базы данных и каталоги журналов и экземпляров на резервный узел кластера PowerHA.

Результаты

Вы должны сконфигурировать устройства хранения со сменными носителями для поддержки отказоустойчивости и задать сервер IBM Spectrum Protect для PowerHA в качестве приложения.

Операционные системы AIX

Конфигурирование сервера IBM Spectrum Protect на основном узле для PowerHA

Можно сконфигурировать экземпляр сервера IBM Spectrum Protect на основном узле.

Процедура

1. Ознакомьтесь с информацией по конфигурированию сервера IBM Spectrum Protect.
2. После того, как вы сконфигурировали экземпляр сервера IBM Spectrum Protect на основном узле, можно сконфигурировать сервер IBM Spectrum Protect на дополнительном узле.

Задачи, связанные с данной:
Конфигурирование экземпляра сервера IBM Spectrum Protect
Операционные системы AIX

Конфигурирование сервера IBM Spectrum Protect на дополнительном узле для PowerHA с общим экземпляром DB2

Если каталог экземпляра DB2 совместно используется узлами в кластере PowerHA, то создавать экземпляр DB2 на дополнительном узле не нужно. Не запускайте мастер dsmicfgx.

Процедура

Чтобы сконфигурировать экземпляр сервера на дополнительном узле с общим экземпляром DB2; сделайте следующее:

1. На каждом узле в кластере добавьте в сценарий /opt/tivoli/tsm/сервер/bin/rc.dsmserv следующий текст:

```
DB2NODES_TEMP='/tmp/db2nodes.tmp'
DB2NODES=${homeDir}/sqllib/db2nodes.cfg
# Текущее имя хоста
HOSTNAME=$(/bin/hostname)
# имя хоста сохранено в db2nodes.cfg
DB2_HOST=$(cat $DB2NODES | cut -d ' ' -f 2)
# если они разные, обновите файл
if [[ "$HOSTNAME" != "$DB2_HOST" ]]
then
  echo "Обновляется имя хоста в db2nodes.cfg"
  sed -e s_${DB2_HOST}_${HOSTNAME}_g $DB2NODES > $DB2NODES_TEMP
  cp $DB2NODES_TEMP $DB2NODES
fi
```

   Совет: Если текст не включен в сценарий, то его можно включить перед запуском сценария /opt/tivoli/tsm/сервер/bin/rc.dsmserv.
2. Переместите все совместно используемые ресурсы на дополнительный узел.
3. Задайте для следующих переменных в сценарии /opt/tivoli/tsm/сервер/bin/startserver указанные значения:

Табл. 1. Переменные в сценарии /opt/tivoli/tsm/сервер/bin/startserver

Описание	Переменная	Пример
Задать в качестве значения INST_USER ID пользователя экземпляра.	INST_USER	INST_USER='tsmuser1'
Задать в качестве значения INST_DIR каталог экземпляра IBM Spectrum Protect. В этом каталоге находятся файлы dsmserv.dbid и dsmserv.opt.	INST_DIR	INST_DIR='/home/tsmuser1/tsminst1'
Выберите одну из следующих опций запуска: Опция 1 - использовать экземпляр: $INST_USER, но запустить сервер как root (-U) Опция 2 - использовать экземпляр: $INST_USER и запустить сервер как $INST_USER (-u)	INST_OPTION	Опция 1: INST_OPTION='-U $INST_USER' Опция 2: INST_OPTION='-u $INST_USER'

4. Запустите сервер, введя следующий сценарий:

```
/opt/tivoli/tsm/server/bin/startserver
```

5. После запуска сервера введите команду BACKUP DB, чтобы убедиться, что данные успешно скопированы.

Операционные системы AIX

Конфигурирование сервера IBM Spectrum Protect на дополнительном узле для PowerHA с отдельным экземпляром DB2

Нужно создать экземпляр DB2 на каждом дополнительном узле, если каталог экземпляра DB2 /home/tsminst1/sqllib не используется узлами совместно в кластере PowerHA.

Об этой задаче

Сервер IBM Spectrum Protect на дополнительном узле можно сконфигурировать при помощи мастера dsmicfgx или вручную.

Процедура

- Чтобы создать экземпляр DB2 на дополнительном узле при помощи мастера dsmicfgx, сделайте следующее:
  1. Запустите мастер dsmicfgx.
  2. В панели Каталог экземпляра выберите переключатель Выберите эту опцию, если вы конфигурируете экземпляр сервера на дополнительном узле или в кластере высокой доступности.
- Чтобы создать экземпляр DB2 на дополнительном узле вручную, сделайте следующее:
  1. Переместите все совместно используемые ресурсы на дополнительный узел.
  2. Создайте экземпляр DB2 командой db2icrt:

     ```
     /opt/tivoli/tsm/db2/instance/db2icrt -s ese -u пользователь_экземпляра
     пользователь_экземпляра
     ```

     где *пользователь_экземпляра* - это пользователь, который владеет экземпляром DB2 на основном узле.
  3. После создания экземпляра DB2 войдите в систему как пользователь экземпляра или при помощи команды su:

     ```
     su - <пользователь_экземпляра>
     ```

  4. От имени пользователя экземпляра введите следующую команду:

     ```
     db2start
     db2 update dbm cfg using DFTDBPATH общий_каталог_бд
     db2 catalog db TSMDB1
     db2stop
     ```

     где *общий_каталог_бд* - это общий каталог базы данных. Обычно общий каталог базы данных - это каталог экземпляра сервера.

Совет: Чтобы определить значение *общий_каталог_бд*, введите на основном узле следующую команду:

```
db2 get dbm cfg | grep DFTDBPATH
```

5. Задайте для следующих переменных в сценарии /opt/tivoli/tsm/сервер/bin/startserver указанные значения:

Табл. 1. Переменные в сценарии /opt/tivoli/tsm/сервер/bin/startserver

Описание	Переменная	Пример
Задать в качестве значения INST_USER ID пользователя экземпляра.	INST_USER	INST_USER='tsmuser1'
Задать в качестве значения INST_DIR каталог экземпляра IBM Spectrum Protect. В этом каталоге находятся файлы dsmserv.dbid и dsmserv.opt.	INST_DIR	INST_DIR='/home/tsmuser1/tsminst1'
Выбрать одну из следующих опций запуска: Опция 1 - использовать экземпляр: $INST_USER, но запустить сервер как root (-U) Опция 2 - использовать экземпляр: $INST_USER и запустить сервер как $INST_USER (-u)	INST_OPTION	Опция 1: INST_OPTION='-U $INST_USER' Опция 2: INST_OPTION='-u $INST_USER'

6. Запустите сервер, введя следующий сценарий:

```
/opt/tivoli/tsm/server/bin/startserver
```

7. После запуска сервера введите команду BACKUP DB, чтобы убедиться, что данные успешно скопированы.

Операционные системы AIX

Установка сервера IBM Spectrum Protect на производственном узле для PowerHA

Установите сервер IBM Spectrum Protect на производственном узле для PowerHA, чтобы можно было сконфигурировать его для кластеризации.

Процедура

Чтобы установить сервер IBM Spectrum Protect на производственном узле для, выполните следующие действия:

1. Установите IBM Spectrum Protect. Выберите один из следующих компонентов:
   - Сервер IBM Spectrum Protect
   - Драйвер устройств IBM Spectrum Protect (если это нужно)
   - Лицензию IBM Spectrum Protect

   Как правило, выполняемые файлы устанавливаются на внутренних дисках производственного узла, а не в совместно используемом дисковом пространстве IBM Spectrum Protect. Выполняемые файлы сервера IBM Spectrum Protect устанавливаются в каталоге /opt/tivoli/tsm/сервер/bin.

2. Сконфигурируйте IBM Spectrum Protect для использования способа связи TCP/IP. Инструкции смотрите в материалах по конфигурированию экземпляра сервера в разделе AIX: Первые шаги после установки IBM Spectrum Protect.
3. Задайте новый ID пользователя, который является владельцем экземпляра сервера IBM Spectrum Protect, или используйте существующий ID пользователя, который еще не является владельцем экземпляра IBM Spectrum Protect. Войдя в систему от имени ID пользователя экземпляра, выполните следующие действия:
   a. Создайте командой mkdir каталог экземпляра в совместно используемой файловой системе, управление которой может принимать на себя резервная система. Этот диск должен быть задан для PowerHA.
   b. Создайте mkdir каталоги базы данных и журналов в совместно используемых файловых системах, управление которыми может принимать на себя резервная система. Эти диски также должны быть заданы в PowerHA для передачи управления в случае сбоя.
   c. Выполните конфигурирование при помощи мастера dsmicfgx.

Задачи, связанные с данной:
AIX: Установка сервера
Обновление сервера
 Операционные системы AIX

Установка клиента IBM Spectrum Protect на производственном узле для PowerHA

Нужно установить только набор файлов клиента резервного копирования и архивирования, содержащий файлы клиента резервного копирования и архивирования и клиента командной строки администрирования.

Процедура

Подробные инструкции по установке клиента IBM Spectrum Protect смотрите в разделе Установка клиентов резервного копирования и архивирования IBM Spectrum Protect.

Выполните следующие действия, чтобы установить клиент IBM Spectrum Protect на производственном узле.

1. Установите выполняемые файлы клиента IBM Spectrum Protect в каталоге /usr/tivoli/tsm/client/ba/bin. Как правило, эти файлы устанавливаются на внутренних дисках производственного узла.
2. Чтобы клиент мог найти сервер, убедитесь, что файл опций сервера dsm.sys указывает на сервер IBM Spectrum Protect. Имя сервера в файле dsm.sys используется только в качестве значения параметра -servername в команде dsmadmc, указывая, с каким сервером следует соединиться.

 Операционные системы AIX

Проверка конфигурации сервера IBM Spectrum Protect для PowerHA

Когда сервер IBM Spectrum Protect будет сконфигурирован для использования PowerHA, необходимо проверить его конфигурацию.

Об этой задаче

При использовании PowerHA все каталоги баз данных, журналов, системы хранения и экземпляров должны находиться на совместно используемых дисках, сконфигурированных для восстановления после отказов с помощью PowerHA.

Процедура

Чтобы определить каталоги на совместно используемом диске, сделайте следующее:

1. Войдите в систему от имени пользователя экземпляра.
2. Запустите сценарий /opt/tivoli/tsm/сервер/bin/dsmclustfs.
3. Изучите файловые системы, о которых сообщено сценарием, и убедитесь, что они расположены на дисках совместного использования. Следующий пример сценария показывает тип информации, с которой вы должны ознакомиться:

```
> su - tsminst1
$ /opt/tivoli/tsm/server/bin/dsmclustfs
SQL1026N  Менеджер базы данных уже активен.
```

При соединении сервера кIBM Spectrum Protect с базой данных DB2 выводится следующая информация о соединении:

```
DB20000I  Команда START DATABASE MANAGER выполнена успешно.

   Информация о соединениях базы данных

 Сервер базы данных = DB2/AIX64 11.1.0
 ID авторизации SQL = TSMINST1
 Локальный алиас базы данных = TSMDB1

Файловые системы для базы данных DB2: /TSMdbspace2 /TSMdbspace1
Файловая система для активного журнала: /TSMalog
```

```
Файловая система для архивного журнала: /TSMarchlog
Зеркальная копия активного журнала на задана для этой базы данных
```

В сценарии присутствуют следующие обязательные файловые системы DB2:

```
 /TSMdb-1 /TSMalog-1 /TSMarchlog-1

Проверка существующих томов на основе диска TSM...
Данные TSM хранятся в следующих файловых системах: /TSMdisk-1 /TSMfile-1
```

 Операционные системы AIX

Как настроить резервный узел для PowerHA

При использовании PowerHA, прежде чем настраивать резервный узел, убедитесь, что сервер IBM Spectrum Protect не работает на производственном узле.

Процедура

Чтобы настроить резервный узел, выполните следующие действия:

1. На резервном узле откройте группу совместно используемых томов и все совместно используемые файловые системы IBM Spectrum Protect.
2. На резервном узле установите код продукта IBM Spectrum Protect. Дополнительные сведения смотрите в разделе Установка сервера IBM Spectrum Protect на производственном узле для PowerHA. Если выполняемые файлы установлены в совместно используемом дисковом пространстве, вам, возможно, потребуется установить их на резервном узле. Драйверы устройств IBM Spectrum Protect, панели SMIT и другие файлы должны быть установлены в системных каталогах AIX.
3. Откройте мастер dsmicfgx. Завершите конфигурирование, следуя инструкциям. Включите переключатель, указывающий, что этот узел - вторичный в кластере.
4. Запустите сервер на резервном узле. Запросите информацию о базе данных, журнале восстановления и томах тома хранения, чтобы убедиться, что они такие же, как и при запуске сервера на производственном узле.
5. Установите клиент на резервном узле. Если выполняемые файлы установлены в совместно используемом дисковом пространстве, вам, возможно, потребуется установить их на резервном узле. Панели SMIT и другие файлы IBM Spectrum Protect должны быть установлены в системных каталогах AIX. Введите команду AIX RCP с опцией -p, чтобы скопировать файл dsm.sys с производственного узла на резервный узел. Если файл dsm.sys изменится на одном узле, его нужно будет скопировать на другой узел.

Результаты

Совет: Если файл dsm.sys изменится на одном узле, вы должны будете скопировать его на другой узел.
 Операционные системы AIX

Как задать устройства хранения со сменными носителями в AIX для PowerHA

В операционной системе AIXнеобходимо определить устройства хранения со сменными носителями, которые используются IBM Spectrum Protect на производственных и резервных узлах. Менеджер библиотеки проверяет, находится ли картридж, содержщий устройство хранения съемного носителя, в правильном накопителе.

Об этой задаче

Требования:

- Если вы определяете сервер менеджера библиотек, который не используется совместно с сервером IBM Spectrum Protect, убедитесь, что для параметра RESETDRIVES команды DEFINE LIBRARY или команды UPDATE LIBRARY задано значение YES. Если вы определяете сервер менеджера библиотеки, который используется совместно с сервером IBM Spectrum Protect, для опции SANDISCOVERY необходимо задать значение ON в файле опций сервера IBM Spectrum Protect dsmserv.opt. По умолчанию для этой опции задано значение OFF.
- Команду PERFORM LIBACTION можно ввести для типов библиотек SCSI и VTL. Используйте эту команду, чтобы за один шаг определить накопители и пути для библиотеки.

Если ваше отображение устройств SAN правильное, перейдите к разделу Завершение конфигурирования менеджера кластера и IBM Spectrum Protect. Если имена устройств в первичной и вторичной системе не совпадают, необходимо использовать процедуру обнаружения SAN, чтобы у сервера IBM Spectrum Protect был доступ к этим устройствам.

Задачи, связанные с данной:
Конфигурирование совместного использования библиотек (V7.1.1)
Ссылки, связанные с данной:
DEFINE LIBRARY (Задать библиотеку)
UPDATE LIBRARY (обновление библиотеки)
PERFORM LIBACTION (Задать или удалить все накопители и пути для библиотеки)
SANDISCOVERY
Информация, связанная с данной:
Поддерживаемые устройства IBM Spectrum Protect
Операционные системы AIX

Завершение конфигурирования менеджера кластера и IBM Spectrum Protect

Измените конфигурацию менеджера кластера, чтобы задать сервер IBM Spectrum Protect как приложение и ресурс переключения после отказа резервного узла. Этим приложением владеет производственный узел.

Об этой задаче

Для настройки кластера можно ввести команды IBM® PowerHA SystemMirror for AIX или System Automation for Multiplatforms. Переходите к конфигурированию сервера IBM Spectrum Protect.

Информация, связанная с данной:
Информация о PowerHA SystemMirror
Информация о IBM Tivoli System Automation for Multiplatforms версии 3.2.2
Операционные системы AIX

Устранение неисправностей кластерной среды PowerHA

Посмотрите в следующем списке информацию об общих проблемах диагностики и устранения неисправностей. В информации, приведенной для IBM® PowerHA SystemMirror for AIX, представлены не все возможные сценарии.

Сообщения с предупреждениями, получаемые после запуска утилиты clverify
: Вы можете запустить утилиту проверки кластера PowerHA clverify на одном узле, чтобы проверить конфигурацию кластера и назначение ресурсов PowerHA. Если запустить утилиту clverify после определения сервера IBM Spectrum Protect как прикладной программы PowerHA, появятся сообщения с предупреждениями.

  Вывод сообщений с предупреждениями обусловлен тем, что сценарии оболочки, запускающие и останавливающие серверы IBM Spectrum Protect, находятся в совместно используемой файловой системе. Сценарии оболочки можно запустить только на одном узле одновременно. Поэтому эти сценарии оболочки могут быть доступны только на одном узле одновременно. Предупреждения утилиты clverify можно игнорировать. Если смонтировать совместно используемую файловую систему невозможно, запустить сервер IBM Spectrum Protect не удастся.

Сервер IBM Spectrum Protect не запускается после запуска сценария startserver
: Если вы используете сценарий startserver и PowerHA не может запустить сервер IBM Spectrum Protect, то запустите его вручную на терминале без опции quiet. Чтобы запустить сервер с опцией quiet, введите команду dsmserv -q.

Сообщения, связанные с командой tctl
: Если ввести команду tctl -f/dev/rmt2 rewind, вы можете получить следующее сообщение:

  ```
  /dev/rmt2: Устройство уже смонтировано или его невозможно размонтировать
  ```

  Это сообщение означает, что устройство ввода-вывода заблокировано при помощи команды SCSI RESERVE какой-то другой системой (а не той, на которой выполнялась команда tctl). Если вы используете постоянное резервирование, у сервера IBM Spectrum Protect по умолчанию есть приоритет резервирования накопителя. Если драйвер устройства не использует постоянное резервирование, сервер выполнит сброс объекта назначения.

Сообщение `ANS4329S На сервере не хватает пространства для хранения данных`

Если на клиенте IBM Spectrum Protect выводится сообщение `ANS4329S На сервере не хватает пространства для хранения данных`, возможно, лицензия для сервера IBM Spectrum Protect не согласована. Введите команду QUERY LICENSE, чтобы показать информацию о соответствии лицензии. Если состояние совместимости допустимо, используйте команду QUERY ACTLOG на сервере и ознакомьтесь с показанными сообщениями, чтобы определить проблему.

 Операционные системы Linux

Конфигурирование среды Linux для кластеризации

Можно сконфигурировать сервер Linux IBM Spectrum Protect в кластерной среде посредством IBM® Tivoli System Automation for Multiplatforms версии 4.1.

-  Операционные системы LinuxОбзор кластера IBM Spectrum Protect с двумя узлами с использованием System Automation for Multiplatforms
  Используйте кластер System Automation for Multiplatforms для повышения доступности сервера и базы данных во время сбоя. При помощи функции переключения после отказа System Automation for Multiplatforms можно автоматически восстановить компоненты сервера (например, базу данных) после отказа.
-  Операционные системы LinuxНастройка кластера IBM Spectrum Protect с помощью System Automation for Multiplatforms
  Нужно настроить кластер IBM Spectrum Protect для использования System Automation for Multiplatforms.
-  Операционные системы LinuxПредварительные требования для конфигурирования кластерной среды Linux с System Automation for Multiplatforms
  Перед установкой и конфигурированием IBM Spectrum Protect в кластерной среде с System Automation for Multiplatforms нужно проверить выполнение обязательных требований.
-  Операционные системы LinuxУстановка и конфигурирование компонентов IBM Spectrum Protect на основном и дополнительном узлах
  Сервер IBM Spectrum Protect и базу данных нужно установить на основном и дополнительном узлах в кластере. После этого сконфигурируйте основной узел, а затем дополнительный.
-  Операционные системы LinuxУстановка System Automation for Multiplatforms на основном и дополнительном узлах
  После установки и конфигурирования IBM Spectrum Protect на основном и дополнительном узлах в кластере нужно установить и сконфигурировать на этих узлах System Automation for Multiplatforms. После этого нужно активировать эти узлы для домена, сконфигурировать ресурсы и активировать базовую политику. Наконец, нужно добавить точки монтирования в каталоги IBM Spectrum Protect.
-  Операционные системы LinuxКонфигурирование ресурсов хранения
  Используйте интерфейс пользователя или командную строку System Automation for Multiplatforms для добавления или удаления ресурсов хранения и для удаления ненужных точек монтирования. Если вы добавляете в кластер пул хранения, то его нужно добавить в группу ресурсов. Если вы удаляете из кластера пул хранения, то его нужно также удалить из группы ресурсов.
-  Операционные системы LinuxОбновление сервера, сконфигурированного компонентом System Automation for Multiplatforms
  Можно обновить сервер, который сконфигурирован с System Automation for Multiplatforms .

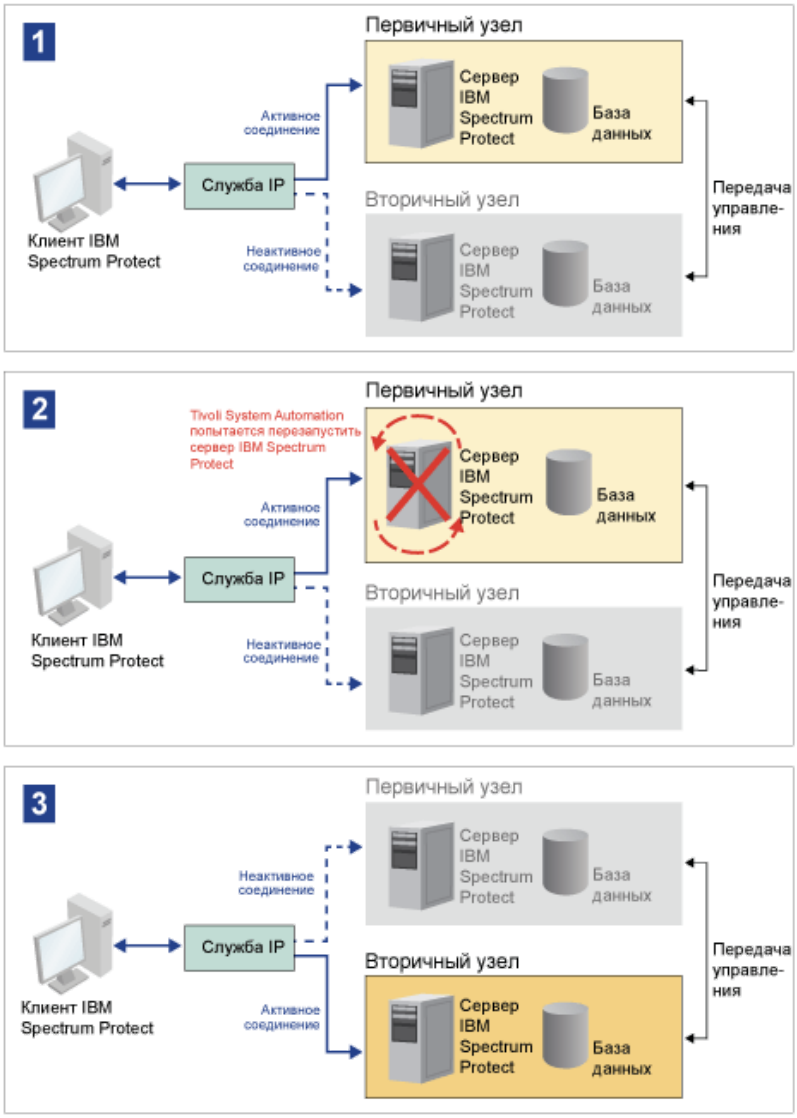
 Операционные системы Linux

Обзор кластера IBM Spectrum Protect с двумя узлами с использованием System Automation for Multiplatforms

Используйте кластер System Automation for Multiplatforms для повышения доступности сервера и базы данных во время сбоя. При помощи функции переключения после отказа System Automation for Multiplatforms можно автоматически восстановить компоненты сервера (например, базу данных) после отказа.

Сервер IBM Spectrum Protect и база данных DB2 - это основные компоненты сервера для такого кластера с двумя узлами. Сервер - это базовый компонент. Он отвечает за операции клиента и сервера. База данных DB2 - это внутренний компонент, который устанавливается как часть сервера. Сервер управляет всеми операциями базы данных (например, запуск и выключение). Если сервер обнаруживает ошибку сервера или базы данных, то он пытается перезапустить базу данных. Если перезапуск завершается неудачно, то сервер и база данных автоматически выключаются на основном узле и System Automation for Multiplatforms автоматически запускает эти компоненты на дополнительном узле. Поскольку функции IBM Spectrum Protect восстанавливаются немедленно, доступность сервера и базы данных возрастает.

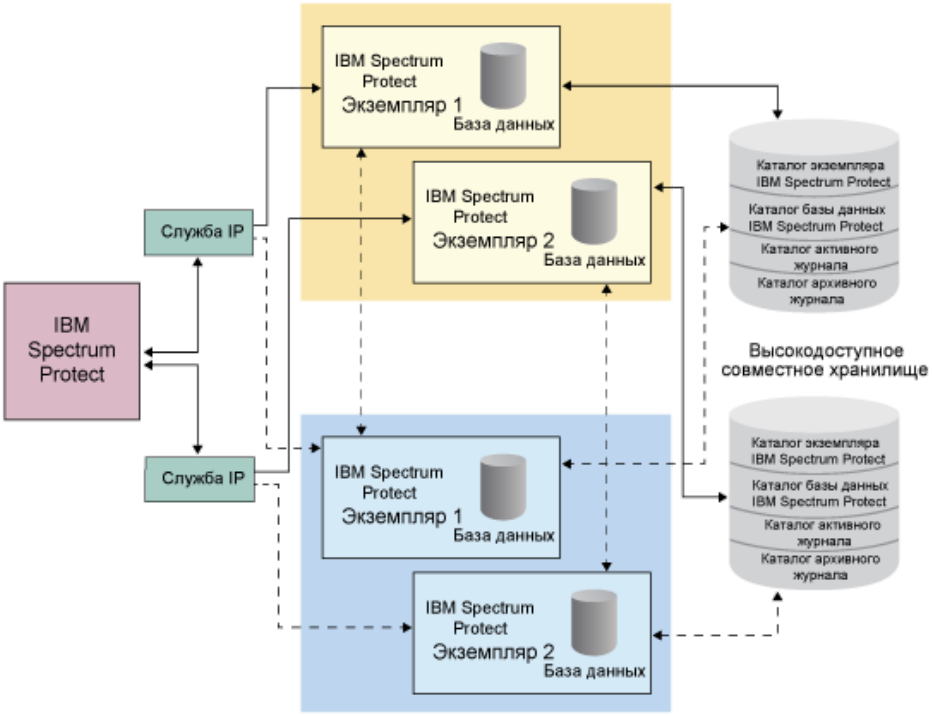
Рис. 1. Функция переключения после отказа. Произошел отказ сервера и базы данных на основном узле. System Automation for Multiplatforms запускает эти компоненты на дополнительном узле.



Сервер и база данных используют для хранения следующие каталоги журнала:

- Каталог экземпляра IBM Spectrum Protect
- Каталог активного журнала
- Каталог архивного журнала
- Каталог базы данных

Два узла в этом кластере System Automation for Multiplatforms сконфигурированы для доступа к высокодоступному совместно используемому хранению, которое защищает данные. Например, топология из двух узлов содержит основной узел и дополнительный узел. Эти узлы находятся на разных физических компьютерах, но могут обращаться к одним и тем же данным с использованием общего массива хранения.
Рис. 2. Несколько экземпляров сервера IBM Spectrum Protect на разных узлах. Эти экземпляры сервера находятся на разных физических компьютерах. Экземпляры могут обращаться к высокодоступному общему хранению.



- Операционные системы LinuxТопология совместно используемого диска с двумя узлами
  В этом кластере используется топология совместно используемого диска с двумя узлами. Она состоит из основного и дополнительного узла. На основном узле находятся сервер IBM Spectrum Protect, база данных, экземпляр IBM Spectrum Protect и данные. Дополнительный узел - это узел, на который перемещаются ресурсы IBM Spectrum Protect, если происходит сбой.
- Операционные системы LinuxГруппы ресурсов System Automation for Multiplatforms
  Используйте группы ресурсов System Automation for Multiplatforms с заданными политиками автоматизации для управления компонентами IBM Spectrum Protect для этого кластера. Единственное исключение - ресурс экземпляра сервера базы данных, который управляется сервером IBM Spectrum Protect.

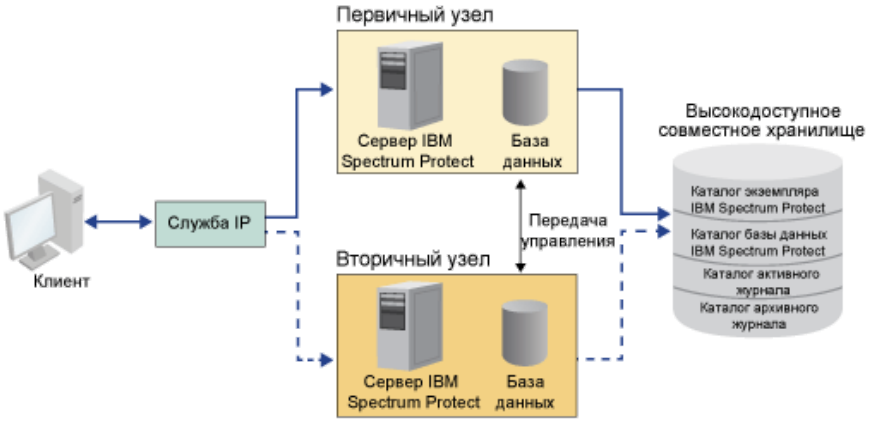
Операционные системы Linux

Топология совместно используемого диска с двумя узлами

В этом кластере используется топология совместно используемого диска с двумя узлами. Она состоит из основного и дополнительного узла. На основном узле находятся сервер IBM Spectrum Protect, база данных, экземпляр IBM Spectrum

Protect и данные. Дополнительный узел - это узел, на который перемещаются ресурсы IBM Spectrum Protect, если происходит сбой.

Два узла в этом кластере соединены друг с другом через одну общедоступную сеть, и подключены к компьютеру *совместно используемого дискового хранения*, который доступен всегда. *Совместно используемое дисковое хранение* - это один или несколько дисков, которые доступны основному и дополнительному узлам. Эти диски всегда смонтированы на одном узле - на основном узле. Один узел может получать данные от совместно используемых дисков хранения и передавать данные на эти диски. На следующем рисунке показана топология с совместным использованием двух узлов с автоматическим переключением на дополнительный узел в случае сбоя экземпляра.



Операционные системы Linux

Группы ресурсов System Automation for Multiplatforms

Используйте группы ресурсов System Automation for Multiplatforms с заданными политиками автоматизации для управления компонентами IBM Spectrum Protect для этого кластера. Единственное исключение - ресурс экземпляра сервера базы данных, который управляется сервером IBM Spectrum Protect.

Совместно используемые файловые системы и компоненты IBM Spectrum Protect задаются как ресурсы. Несколько ресурсов составляют группу ресурсов. У каждого ресурса в группе ресурсов есть тип. В состав каждого экземпляра IBM Spectrum Protect в кластере входит группа ресурсов. Во время запланированных остановок группы ресурсов можно вручную переместить из основного узла на дополнительный.

В группу ресурсов IBM Spectrum Protect входят следующие ресурсы. Имя группы ресурсов IBM Spectrum Protect - SA-tsm-inst1-rg, где inst1 - это имя экземпляра. Для разных, но обязательных функций в этом кластере используются следующие ресурсы:

IP службы
: Ресурс IP службы используется для связи. Он называется tsm-inst1-ip-rs, где inst1 - это имя экземпляра. IP службы управляется System Automation for Multiplatforms. Этот IP доступен на узле, на котором работает сервер IBM Spectrum Protect. Нужно создать логический интерфейс IP службы в том же физическом интерфейсе, что и общедоступный интерфейс сети.

Ресурс *совместно используемого дискового хранения*
: Ресурс *совместно используемого дискового хранения* - это физическое устройство хранения на сервере IBM Spectrum Protect, на котором хранятся данные IBM Spectrum Protect и приложения DB2. Нужно создать следующие ресурсы дискового хранения:

  - Каталог экземпляра - tsm inst1 instdir ag
  - Каталог DB2 - tsm-inst1-db2dir-ag
  - Каталог активного журнала - tsm-inst1-actlog-ag
  - Каталог архивного журнала - tsm-inst1-archlog-ag

Совместно используемое дисковое хранение для пулов хранения

В ресурс пула хранения входят физические устройства хранения на сервере IBM Spectrum Protect, на котором хранятся данные клиента.

Ресурсы группы томов
: Если вы решили сконфигурировать свое хранение с использованием групп томов, то для работы предшествующих ресурсов *совместно используемого дискового хранения* доступен ресурс группы томов. Ресурсы группы томов автоматически создаются System Automation for Multiplatforms.

Ресурсы приложений для экземпляра сервера IBM Spectrum Protect
: Ресурс экземпляра сервера IBM Spectrum Protect - это ресурс сервера, который управляет приложением IBM Spectrum Protect. Этот ресурс управляется сценариями управления System Automation for Multiplatforms.

Табл. 1. Задачи, выполняемые сценариями управления System Automation for Multiplatforms

Задачи	Описание	Примеры команд
Начало	Запускает экземпляр сервера IBM Spectrum Protect.	Команда /opt/tivoli/tsm/server/bin/rc.dsmserv -u db2inst1 –i /tsminst1 запускает экземпляр сервера с пользователем db2inst1 в каталоге /tsminst1.
Стоп	Останавливает экземпляр сервера IBM Spectrum Protect.	kill –s SIGURG 345, где `345` - это *PID*. Значение *PID* указано в файле /tsminst1/dsmserv.v6lock.
Наблюдатель	Проверяет, существует ли файл /tsminst1/dsmserv.v6lock. Для проверки работы процесса используется *PID*.	ps -ef | grep 345, где `345` - это *PID*.

- Операционные системы LinuxЗависимости групп ресурсов
  Зависимости групп ресурсов автоматически создаются для управления последовательностью запуска ресурсов. Эти зависимости также задают, какие ресурсы нужно перезапустить или выключить при сбое конкретного ресурса, от которого зависят эти ресурсы.

Операционные системы Linux

Настройка кластера IBM Spectrum Protect с помощью System Automation for Multiplatforms

Нужно настроить кластер IBM Spectrum Protect для использования System Automation for Multiplatforms.

Процедура

1. Установите и сконфигурируйте компоненты IBM Spectrum Protect на основном и дополнительном узлах.
2. Установите System Automation for Multiplatforms на основном и дополнительном узлах.
3. Сконфигурируйте ресурсы хранения.
4. В зависимости от версии IBM Spectrum Protect, установленной на сервере, возможно, придется обновить сервер IBM Spectrum Protect для кластера System Automation for Multiplatforms.
5. Необязательно: Можно задать переменную *FILE_EXIT* в кластерном сценарии tsmserverctrl, чтобы маршрутизировать данные событий System Automation for Multiplatforms в файл FILEEXIT сервера IBM Spectrum Protect.
   Например, измените сценарий кластера tsmserverctrl в каталоге *<каталог_установки_сервера>*/tsam/controls, добавив в него следующую строку:

   ```
   FILE_EXIT="fileexittmp"
   ```

Операционные системы Linux

Предварительные требования для конфигурирования кластерной среды Linux с System Automation for Multiplatforms

Перед установкой и конфигурированием IBM Spectrum Protect в кластерной среде с System Automation for Multiplatforms нужно проверить выполнение обязательных требований.

Сделайте следующее:

- Запланируйте установку сервера IBM Spectrum Protect. Дополнительную информацию смотрите в разделе Установка and обновление сервера.
- Подготовьтесь к установке System Automation for Multiplatforms. Инструкции смотрите в документации по продукту System Automation for Multiplatforms. В публикации *Руководство по установке и конфигурированию*, найдите раздел *Подготовка к установке*.

Задачи, связанные с данной:
Планирование установки сервера IBM Spectrum Protect
 Операционные системы Linux

Установка и конфигурирование компонентов IBM Spectrum Protect на основном и дополнительном узлах

Сервер IBM Spectrum Protect и базу данных нужно установить на основном и дополнительном узлах в кластере. После этого сконфигурируйте основной узел, а затем дополнительный.

-  Операционные системы LinuxУстановка компонентов сервера IBM Spectrum Protect
  После проверки предварительных требований необходимо установить необходимые компоненты IBM Spectrum Protect.
-  Операционные системы LinuxКонфигурирование основного узла
  Чтобы настроить топологию с двумя узлами, сконфигурируйте компоненты IBM Spectrum Protect на обоих узлах. Вначале нужно сконфигурировать экземпляр IBM Spectrum Protect на основном узле.
-  Операционные системы LinuxКонфигурирование дополнительного узла
  После конфигурирования основного узла нужно сконфигурировать дополнительный узел, чтобы System Automation for Multiplatforms мог переместить компоненты сервера IBM Spectrum Protect на дополнительный узел в случае отказа сервера на основном узле.

 Операционные системы Linux

Установка компонентов сервера IBM Spectrum Protect

После проверки предварительных требований необходимо установить необходимые компоненты IBM Spectrum Protect.

Процедура

Установите сервер IBM Spectrum Protect на основных (первичных) и вторичных узлах.
Задачи, связанные с данной:
Установка компонентов сервера IBM Spectrum Protect
 Операционные системы Linux

Конфигурирование основного узла

Чтобы настроить топологию с двумя узлами, сконфигурируйте компоненты IBM Spectrum Protect на обоих узлах. Вначале нужно сконфигурировать экземпляр IBM Spectrum Protect на основном узле.

Прежде чем начать

- Убедитесь, что на всех узлах в домене кластера для владельца экземпляра IBM Spectrum Protect заданы одинаковые ID пользователя и группы.
- Убедитесь, что на всех узлах кластера для владельца экземпляра IBM Spectrum Protect задан один и тот же пароль.

Процедура

1. Подробные инструкции по созданию каталогов и ID пользователей для экземпляра сервера смотрите в разделе Linux: Создание ID пользователей и каталогов для экземпляра сервера.

2. Убедитесь, что сервер IBM Spectrum Protect, экземпляр DB2, каталоги активного и архивного журналов и каталог зеркального журнала, если это применимо, являются совместно используемыми.
3. Задайте точки монтирования, добавив записи в файл /etc/fstab.

   При добавлении точек монтирования в узлы кластера укажите опцию noauto, чтобы предотвратить автоматическое монтирование точек монтирования на нескольких узлах в кластере.

4. Задайте в каждой из точек монтирования следующие разрешения:
   - 755. Например, следующая команда задает разрешение 755 в точке монтирования `/tsminst1`:

     ```
     chmod -R 755 /tsminst1
     ```

   - Владелец экземпляра сервера IBM Spectrum Protect. Например, следующая команда задает разрешения для владельца экземпляра:

     ```
     chown -R  tsminst1  /tsminst1
     ```

   - Группа сервера IBM Spectrum Protect, в которую входит владелец экземпляра. Например, следующая команда задает разрешения для группы владельцев экземпляра:

     ```
     chgrp tsmsrv_1_group /tsminst1
     ```

5. Смонтируйте общие ресурсы.
6. Войдите в основной узел, используя ID пользователя экземпляра. Перейдите в каталог экземпляра и запустите экземпляр сервера IBM Spectrum Protect на первичном узле утилитой DSMSERV. Например, следующая команда запускает сервер для обычной работы:

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

7. Убедитесь, что компоненты IBM Spectrum Protect запускаются без ошибок.
8. Остановите сервер IBM Spectrum Protect.
9. Войдите в систему с ID пользователя root и размонтируйте общие диски.

 Операционные системы Linux

Конфигурирование дополнительного узла

После конфигурирования основного узла нужно сконфигурировать дополнительный узел, чтобы System Automation for Multiplatforms мог переместить компоненты сервера IBM Spectrum Protect на дополнительный узел в случае отказа сервера на основном узле.

Процедура

1. Чтобы создать каталоги и ID пользователя для экземпляра сервера вручную, выполните инструкции из раздела Создание ID пользователей и каталогов для экземпляра сервера. Убедитесь, что на основном и дополнительном узлах используются одни и те же имена каталогов.
2. Задайте точки монтирования, добавив записи в файл /etc/fstab.

   При добавлении точек монтирования в узлы кластера укажите опцию noauto. Эта опция предотвращает автоматическое монтирование точек монтирования на нескольких узлах в кластере.

   Убедитесь, что идентификаторы UID дисков для каждого монтирования соответствуют UID дисков на основном узле.
3. Задайте в каждой из точек монтирования следующие разрешения:
   - 755. Например, следующая команда задает разрешение 755 в точке монтирования `/tsminst1`:

     ```
     chmod -R 755 /tsminst1
     ```

   - Владелец экземпляра сервера IBM Spectrum Protect. Например, следующая команда задает разрешения для владельца экземпляра:

     ```
     chown -R  tsminst1  /tsminst1
     ```

   - Группа сервера IBM Spectrum Protect, в которую входит владелец экземпляра. Например, следующая команда задает разрешения для группы владельцев экземпляра:

     ```
     chgrp tsmsrv_1_group /tsminst1
     ```

4. Смонтируйте общие диски.
5. Создайте экземпляр сервера IBM Spectrum Protect, введя команду db2icrt. Инструкции смотрите в разделе Создание экземпляра сервера.
   Напоминание: Вам не нужно создавать новый файл опций сервера, потому что вторичный узел использует файл dsmserv.opt с первичного узла.
6. Войдите во вторичный узел, используя ID пользователя экземпляра. Каталогизируйте базу данных командой catalog db. Например, следующая команда каталогизирует базу данных `tsmdb1`:

   ```
   db2 catalog db tsmdb1
   ```

7. Подготовьте базу данных для резервного копирования. Инструкции смотрите в разделе Подготовка менеджера базы данных к резервному копированию базы данных.
8. Перейдите в каталог экземпляра и запустите сервер IBM Spectrum Protect утилитой DSMSERV. Например, следующая команда запускает сервер для обычной работы:

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

9. Убедитесь, что компоненты IBM Spectrum Protect запускаются без ошибок.
10. Остановите сервер IBM Spectrum Protect и размонтируйте совместно используемые каталоги.

Операционные системы Linux

Установка System Automation for Multiplatforms на основном и дополнительном узлах

После установки и конфигурирования IBM Spectrum Protect на основном и дополнительном узлах в кластере нужно установить и сконфигурировать на этих узлах System Automation for Multiplatforms. После этого нужно активировать эти узлы для домена, сконфигурировать ресурсы и активировать базовую политику. Наконец, нужно добавить точки монтирования в каталоги IBM Spectrum Protect.

- Операционные системы LinuxСоздание меток для точек монтирования
  Создайте метку для каждой точки монтирования на основных и дополнительных узлах в кластере.
- Операционные системы LinuxУстановка и конфигурирование System Automation for Multiplatforms
  Сервер IBM Spectrum Protect можно интегрировать с IBM Tivoli System Automation for Multiplatforms in в кластерной среде. Используя функцию отказоустойчивости System Automation for Multiplatforms, можно убедиться, что компоненты сервера IBM Spectrum Protect автоматически восстанавливаются после ошибок.
- Операционные системы LinuxПодготовка к активации узлов кластера для домена
  После установки System Automation for Multiplatforms на основном и дополнительном узлах в кластере нужно подготовить эти узлы, чтобы можно было активировать кластер и запустить домен кластера.
- Операционные системы LinuxКонфигурирование ресурсов группы томов
  Если вы создали группы томов для вашего кластера, вы должны сконфигурировать эти ресурсы. System Automation for Multiplatforms автоматически находит и определяет ресурсы тома совместно используемого диска.
- Операционные системы LinuxКонфигурирование ресурсов, не входящих в группу томов
  Если вы создали ресурсы *совместно используемого дискового хранения* с использованием типов ресурсов ext2, ext3 или reiserfs на одном из узлов в кластере, то нужно сконфигурировать эти ресурсы.
- Операционные системы LinuxАктивация базовой политики
  После конфигурирования ресурсов нужно активировать политику на основном и дополнительном узлах, чтобы создать все остальные ресурсы и группы ресурсов.
- Операционные системы LinuxДобавление точек монтирования в каталоги IBM Spectrum Protect
  Перед запуском кластера нужно добавить точки монтирования, созданные для компонентов IBM Spectrum Protect.

Операционные системы Linux

Создание меток для точек монтирования

Создайте метку для каждой точки монтирования на основных и дополнительных узлах в кластере.

Процедура

1. Создайте метку для каждого из томов, которые вы создали ранее для точек монтирования общего каталога, при помощи команды e2label. Например, следующая команда создает метку /tsminst1 для раздела /dev/tsmvg1/tsminst1LV.

```
e2label /dev/tsmvg1/tsminst1LV /tsminst1
```

2. Для каждого узла в кластере создайте запись e2label для точек монтирования, которые вы создали ранее в файле /etc/fstab. Например, для предыдущего примера метки введите следующую команду:

```
LABEL=/tsminst1 /tsminst1 ext3 defaults 0 0
```

 Операционные системы Linux

Установка и конфигурирование System Automation for Multiplatforms

Сервер IBM Spectrum Protect можно интегрировать с IBM® Tivoli System Automation for Multiplatforms in в кластерной среде. Используя функцию отказоустойчивости System Automation for Multiplatforms, можно убедиться, что компоненты сервера IBM Spectrum Protect автоматически восстанавливаются после ошибок.

Прежде чем начать

Выполните следующие задачи:

1. Убедитесь, что вы имеете представление об основных терминах, понятиях и компонентах, связанных с System Automation for Multiplatforms. Дополнительные сведения смотрите в разделе Компоненты.
2. Получите базовый выпуск System Automation for Multiplatforms с сайта Passport Advantage и скачайте последний уровень обслуживания с сайта Fix Central.
3. Установите и сконфигурируйте System Automation for Multiplatforms, следуя инструкциям в публикации *Руководство по установке и конфигурированию*.

Процедура

1. Чтобы интегрировать System Automation for Multiplatforms с IBM Spectrum Protect, следуйте инструкциям в техническом замечании 7039780. Настройте хотя бы один кластер, в котором есть хотя бы два узла.
2. Проверьте конфигурацию, чтобы убедиться, что все каталоги базы данных, журналов, хранения и экземпляров находятся на совместно используемых дисках, сконфигурированных для отказоустойчивости. Выполните следующие действия.
    a. Войдите в систему от имени пользователя экземпляра.
    b. Запустите сценарий /opt/tivoli/tsm/server/bin/dsmclustfs и смотрите выходную информацию. Убедитесь, что файловые системы, о которых сообщает сценарий, находятся на совместно используемых дисках.
3. Проверьте кластерную среду, используя процедуры в техническом замечании 7039780. Убедитесь, что функции отказоустойчивости действуют так, как ожидается.

Информация, связанная с данной:
Информация о IBM Tivoli System Automation for Multiplatforms версии 4.1
Операционные системы Linux

Подготовка к активации узлов кластера для домена

После установки System Automation for Multiplatforms на основном и дополнительном узлах в кластере нужно подготовить эти узлы, чтобы можно было активировать кластер и запустить домен кластера.

Процедура

1. Подготовьте каждый узел для домена, введя команду preprpnode. Введите эту команду для всех узлов кластера в домене. Например, следующая команда готовит узлы HOST1.ibm.com и HOST2.ibm.com:

```
preprpnode HOST1.ibm.com HOST2.ibm.com
```

2. Создайте домен с помощью команды mkrpdomain. Например, следующая команда создает домен tsm_domain для узлов HOST1.ibm.com и HOST2.ibm.com:

```
mkrpdomain tsm_domain HOST1.ibm.com HOST2.ibm.com
```

3. Запустите домен для каждого узла, введя команду startrpdomain. Например, следующая команда запускает tsm_domain:

```
startrpdomain tsm_domain
```

Операционные системы Linux

Конфигурирование ресурсов группы томов

Если вы создали группы томов для вашего кластера, вы должны сконфигурировать эти ресурсы. System Automation for Multiplatforms автоматически находит и определяет ресурсы тома совместно используемого диска.

Процедура

Чтобы сконфигурировать ресурсы группы томов для совместно используемых каталогов IBM Spectrum Protect и точек монтирования, созданных ранее, сделайте на основном узле следующее:

1. Импортируйте группы томов. Например, используйте команду vgimport X для импорта группы томов `X`.
2. Активируйте группы томов. Например, используйте команду vgchange X для активации группы томов `X`.
3. Смонтируйте файловую систему при помощи команды mount. В следующем примере монтируется файловая система `X`.

   ```
   mount X
   ```

4. Перезапустите домен при помощи команд stoprpdomain и startrpdomain. Например, следующие команды перезапускают tsm_domain.

   ```
   stoprpdomain tsm_domain
   startrpdomain tsm_domain
   ```

5. Размонтируйте файловую систему при помощи команды umount. Например, используйте команду umount X для размонтирования файловой системы `X`.
6. Деактивируйте группы томов. Например, используйте команду vgchange X для деактивации группы томов `X`.
7. Убедитесь, что все ресурсы хранения IBM®.AgfileSystem собираются System Automation for Multiplatforms; для этого введите следующую команду:

   ```
   lsrsrc –s “Name==’Resource_Name' && ResourceType=1” IBM.AgFileSystem
   ```

Операционные системы Linux

Конфигурирование ресурсов, не входящих в группу томов

Если вы создали ресурсы *совместно используемого дискового хранения* с использованием типов ресурсов ext2, ext3 или reiserfs на одном из узлов в кластере, то нужно сконфигурировать эти ресурсы.

Процедура

Сделайте на основном узле следующее:

1. Смонтируйте файловую систему при помощи команды mount. Например, следующая команда монтирует файловую систему `X`.

   ```
   mount X
   ```

2. Перезапустите домен при помощи команд stoprpdomain и startrpdomain. Например, следующая команда перезапускает tsm_domain.

   ```
   stoprpdomain tsm_domain
   startrpdomain tsm_domain
   ```

3. Размонтируйте файловую систему при помощи команды umount. Например, следующая команда размонтирует файловую систему `X`.

   ```
   umount X
   ```

4. Убедитесь, что все ресурсы хранения IBM®.AgfileSystem собираются System Automation for Multiplatforms; для этого введите следующую команду:

   ```
   lsrsc –s “Name==’Resource_Name' && ResourceType=1” IBM.AgFileSystem
   ```

Например, чтобы проверить ресурс *tsmalog*, введите следующую команду:

```
lsrsrc -s "Name=='tsmalog' && ResourceType=1" IBM.AgFileSystem
      Хранимые атрибуты ресурса для ресурса IBM.AgFileSystem 1:
      ResourceHandle= "0x2038 0xffff 0x6ad47197 0x256fc23d 0x9338a9950x263fa510"
      Name                = "tsmalog"
      ResourceType        = 1   <------------------------------
      MountPoint          = ""
      DeviceName          = ""
      Vfs                 = "ext3"
      AggregateResource   = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000 0x00000000"
      ContainerResource   = "0x2036 0xffff 0x6ad47197 0x256fc23d 0x9338a995 0x25ffaa28"
      GhostDevice         = 0
      ResourceId          = "360050768019c021d30000000000005da"
      ProtectionMode      = 1
      UserControl         = 0
      SysMountPoint       = "/tsmalog"
      Label               = "/tsmalog"
      FSID                = "5792f887-8547-4c33-a519-9d0c50ab6882"
      PreOnlineMethod     = 0
      ContainerResourceId = "360050768019c021d30000000000005da"
      AutoMonitor         = 1
      Options             = "defaults,noauto"
      PreOfflineMethod    = 0
      ActivePeerDomain    = "TSM_Domain"
      NodeNameList        =
{"tsmlnode01.storage.tucson.ibm.com","tsmlnode02.storage.tucson.ibm.com"}
```

Операционные системы Linux

Активация базовой политики

После конфигурирования ресурсов нужно активировать политику на основном и дополнительном узлах, чтобы создать все остальные ресурсы и группы ресурсов.

Об этой задаче

Для активации базовой политики нужно создать ресурс IP службы и ресурсы приложения IBM Spectrum Protect для экземпляра сервера IBM Spectrum Protect. После этого нужно создать группу ресурсов и политики для управления кластером.

Процедура

Выполните на всех узлах кластера следующие шаги:

1. Перейдите в каталог /opt/tivoli/tsm/server/bin/tsam/bin.
2. Измените в сценарии base_cluster_variables.sh следующие переменные:
   - *NODE1* задает имя хоста для узла 1 (первичный узел) в кластере.
   - *NODE2* задает имя хоста для узла 2 (дополнительный узел) в кластере.
   - *IP_GATEWAY* задает шлюз IP службы.
   - *SUBNET_MASK* задает маску подсети IP службы.
   - *NET_INT* задает имя сетевой карты конкретного узла в кластере. Это имя должно быть одинаковым для всех узлов в кластере.
3. Запустите сценарий конфигурирования configureHA.sh при помощи команды ./configureHA.sh на всех узлах в кластере.
   Если сценарий configureHA.sh завершается неудачно с ошибкой `-bash: ./configureHA.sh: /bin/bash^M: bad interpreter: No such file or directory`, то введите команду dos2unix для всех сценариев в каталоге bin. Например, для каждого сценария введите следующую команду:

   ```
   dos2unix -o <имя_файла>
   ```

4. Убедитесь, что конфигурирование выполнено успешно: проверьте, выполняются ли сценарии конфигурирования.
5. Внимание: Это действие нужно выполнить только на основном узле.
   Запустите сценарий конфигурирования, введя команду ./setup.sh. Например, следующая команда запускает сценарий конфигурирования на экземпляре `inst1` сервера IBM Spectrum Protect для пользователя экземпляра `dbinst1` в каталоге экземпляра сервера IBM Spectrum Protect `/tsminst1` с IP службы `9.11.142.129`.

```
./setup.sh inst1 dbinst1 /tsminst1 9.11.142.129
```

6. Убедитесь, что группа ресурсов IP создана, выполнив следующую команду:

   ```
   lssam -V
   ```

7. Повторите шаг 3 для всех экземпляров IBM Spectrum Protect в среде сервера IBM Spectrum Protect.

Операционные системы Linux

Добавление точек монтирования в каталоги IBM Spectrum Protect

Перед запуском кластера нужно добавить точки монтирования, созданные для компонентов IBM Spectrum Protect.

Процедура

Чтобы добавить точки монтирования общего диска в группу ресурсов кластера и подключить кластер, сделайте следующее:

1. Определите точки монтирования для следующих каталогов:
   - Экземпляр
   - Database
   - Активный журнал
   - Архивный журнал
   - Пул хранения
2. Добавьте ресурсы в каждую точку монтирования:
   a. Проверьте, подключена ли группа ресурсов tsm-$INST_NAME-rg: введите команду lssam.
   b. Если группа ресурсов tsm-$INST_NAME-rg подключена, то отключите ее, введя следующую команду:

      ```
      chrg -o offline tsm-$INST_NAME-rg
      ```

   c. Добавьте ресурсы общего диска в каждую точку монтирования, запустив сценарий ./update_setup.sh. Например, следующая команда добавляет точку монтирования `/tsminst1` в экземпляр `inst1` сервера IBM Spectrum Protect.

      ```
      ./update_setup.sh inst1 /tsminst1
      ```

3. Подключите группу ресурсов tsm-$INST_NAME-rg, введя следующую команду:

   ```
   chrg -o online tsm-$INST_NAME-rg
   ```

4. Соединитесь с сервером, используя IP-адрес шлюза службы, чтобы убедиться, что конфигурация является правильной.

Операционные системы Linux

Конфигурирование ресурсов хранения

Используйте интерфейс пользователя или командную строку System Automation for Multiplatforms для добавления или удаления ресурсов хранения и для удаления ненужных точек монтирования. Если вы добавляете в кластер пул хранения, то его нужно добавить в группу ресурсов. Если вы удаляете из кластера пул хранения, то его нужно также удалить из группы ресурсов.

- Операционные системы LinuxДобавление пула хранения в группу ресурсов
  Если в конфигурации IBM Spectrum Protect данные хранятся на дисках, то нужно добавить точку монтирования общего диска для пула хранения в группу ресурсов.
- Операционные системы LinuxУдаление пула хранения из группы ресурсов
  Можно удалить пул хранения, который больше не нужен. Если пул хранения удаляется из экземпляра сервера IBM Spectrum Protect, то его нужно удалить из группы ресурсов.
- Операционные системы LinuxУдаление точки монтирования из группы ресурсов
  Можно удалить точку монтирования, которая больше не нужна.

Операционные системы Linux

Добавление пула хранения в группу ресурсов

Если в конфигурации IBM Spectrum Protect данные хранятся на дисках, то нужно добавить точку монтирования общего диска для пула хранения в группу ресурсов.

Процедура

Чтобы добавить в группу ресурсов точку монтирования общего диска для пула хранения, сделайте следующее:

1. Заблокируйте группу ресурсов, введя команду rgreq -o lock. Например, следующая команда блокирует группу ресурсов `Sample_Resourcegroup_X`:

   ```
   rgreq -o lock Sample_Resourcegroup_X
   ```

2. Перейдите в каталог /opt/tivoli/tsm/server/bin/tsam/bin.
3. Чтобы добавить в группу ресурсов ресурс пула хранения, запустите сценарий update_setup.sh командой ./update_setup.sh. Например, следующая команда добавляет точку монтирования пула хранения `/inst1stg1` в экземпляр `inst1` сервера IBM Spectrum Protect:

   ```
   ./update_setup.sh inst1 /inst1stg1
   ```

4. Разблокируйте группу ресурсов, введя команду rgreq -o unlock. Например, следующая команда разблокирует группу ресурсов `Sample_Resourcegroup_X`:

   ```
   rgreq -o unlock Sample_Resourcegroup_X
   ```

 Операционные системы Linux

Удаление пула хранения из группы ресурсов

Можно удалить пул хранения, который больше не нужен. Если пул хранения удаляется из экземпляра сервера IBM Spectrum Protect, то его нужно удалить из группы ресурсов.

Процедура

Чтобы удалить пул хранения, сделайте следующее:

1. Заблокируйте группу ресурсов, введя команду rgreq -o lock. Например, следующая команда блокирует группу ресурсов `Sample_Resourcegroup_X`.

   ```
   rgreq -o lock Sample_Resourcegroup_X
   ```

2. Перейдите в каталог bin при помощи команды cd.
3. Чтобы удалить из группы ресурсов ресурс пула хранения, запустите сценарий delete_mount.sh командой ./delete_mount.sh. Например, следующая команда удаляет точку монтирования `/inst1stg1` из экземпляра `inst1` сервера IBM Spectrum Protect.

   ```
   ./delete_mount.sh /inst1stg1 inst1
   ```

4. Разблокируйте группу ресурсов, введя команду rgreq -o unlock. Например, следующая команда разблокирует группу ресурсов `Sample_Resourcegroup_X`.

   ```
   rgreq -o unlock Sample_Resourcegroup_X
   ```

 Операционные системы Linux

Удаление точки монтирования из группы ресурсов

Можно удалить точку монтирования, которая больше не нужна.

Процедура

Чтобы удалить точку монтирования, сделайте следующее:

1. Проверьте, подключена ли группа ресурсов tsm-$INST_NAME-rg: введите команду lssam.
2. Если группа ресурсов tsm-$INST_NAME-rg подключена, то отключите ее, введя следующую команду:

   ```
   chrg -o offline tsm-$INST_NAME-rg
   ```

3. Перейдите в каталог bin при помощи команды cd.
4. Чтобы удалить точку монтирования, запустите сценарий delete_mount.sh. Например, следующая команда удаляет точку монтирования `/tsminst1` из группы ресурсов экземпляра `inst1` сервера IBM Spectrum Protect.

   ```
   ./delete_mount.sh /tsminst1 inst1
   ```

5. Подключите группу ресурсов tsm-$INST_NAME-rg, введя следующую команду:

   ```
   chrg -o online tsm-$INST_NAME-rg
   ```

 Операционные системы Linux

Обновление сервера, сконфигурированного компонентом System Automation for Multiplatforms

Можно обновить сервер, который сконфигурирован с System Automation for Multiplatforms .

Процедура

Чтобы обновить сервер на каждом узле кластера, войдите в систему на сервере и выполните описанные ниже действия. Эти действия запускают обновление на первичном (основном) узле, а затем - на вторичном.

1. Остановите ресурсы сервера, введя команду chrg -o Offline. Например, следующая команда останавливает ресурсы в группе ресурсов tsm-tsminst1-rg:

   ```
   chrg -o Offline tsm-tsminst1-rg
   ```

2. Остановите домен System Automation for Multiplatforms, введя команду stoprpdomain. Например, следующая команда останавливает tsm_domain:

   ```
   stoprpdomain tsm_domain
   ```

3. Смонтируйте точки монтирования сервера на первичном узле.
4. Информацию об обновлении сервера на первичном узле смотрите в разделе Обновление IBM Spectrum Protect.
5. После завершения обновления выполните действия пост-обновления, чтобы убедиться, что обновление на первичном узле выполнено успешно.
6. Остановите сервер и размонтируйте точки монтирования на первичном узле.
7. Смонтируйте точки монтирования сервера на вторичном узле.
8. Если вы обновляете сервер версии V6 до V7, выполните следующие действия:
   a. Деинсталлируйте сервер.

      Инструкции смотрите в разделе Деинсталляция сервера V6.3 (смотрите *Руководство по установке)*.

   b. Установите сервер на вторичном узле. Следуйте инструкциям в разделе Linux: Установка компонентов сервера.
9. Информацию об обновлении сервера на дополнительном узле смотрите в разделе Обновление сервера.
10. После завершения обновления выполните действия пост-обновления, чтобы убедиться, что обновление на дополнительном узле выполнено успешно.
11. Размонтируйте точки монтирования сервера на вторичном узле.
12. Запустите домен System Automation for Multiplatforms, введя команду startrpdomain. Например, следующая команда запускает tsa_domain:

    ```
    startrpdomain tsa_domain
    ```

13. Запустите ресурсы сервера, введя команду chrg -o Online. Например, следующая команда запускает ресурсы в группе ресурсов tsm-tsminst1-rg:

    ```
    chrg -o Online tsm-tsminst1-rg
    ```

 Операционные системы Windows

Конфигурирование кластерной среды Windows

Вы можете сконфигурировать сервер IBM Spectrum Protect для Windows в среде Microsoft Failover Cluster. Кластерные среды Windows состоят из следующих компонентов: серверов IBM Spectrum Protect, аппаратных компонентов и программного обеспечения. Когда эти компоненты соединены с одной дисковой системой, время простоя минимизируется.

Программное обеспечение Microsoft помогает производить конфигурирование и мониторинг программных и аппаратных компонентов, внедренных в кластере Windows, а также управлять ими. Администратор использует для организации кластеров и определения обработки отказов интерфейс Microsoft Cluster Administrator и IBM Spectrum Protect.

IBM Spectrum Protect поддерживает обработку отказов ленточных устройств для кластеризованных сред с использованием оптоволоконного или SCSI-соединения. Хотя Microsoft Failover Cluster не поддерживает обработку отказов ленточных устройств, конфигурацию передачи управления можно отслеживать через интерфейс Microsoft Cluster Administrator после его установки через IBM Spectrum Protect.

- Операционные системы WindowsОбзор среды Microsoft Failover Cluster
  Microsoft Failover Cluster Manager позволяет поместить кластерные ресурсы сервера IBM Spectrum Protect в группу кластера. Группа кластера IBM Spectrum Protect имеет сетевое имя, IP-адрес, один или несколько физических дисков, сервер DB2 и службу сервера IBM Spectrum Protect.
- Операционные системы WindowsОтказоустойчивость ленточных устройств для узлов в кластере
  Если на узле, который является хостом для группы в кластере, произойдет сбой, группу можно будет перенести на другие узлы.
- Операционные системы WindowsПланирование кластерной среды
  Планирование при конфигурировании в кластерной среде помогает обеспечить оптимальную производительность используемой системы. Необходимость конфигурирования системы для использования кластеров зависит от потребностей вашего предприятия.
- Операционные системы WindowsКонфигурирование IBM Spectrum Protect в кластере Microsoft Failover Cluster
  Перед установкой IBM Spectrum Protect надо убедиться, что кластер правильно установлен и сконфигурирован.
- Операционные системы WindowsУправление кластерной средой
  После настройки первоначального кластера или кластеров потребности в обслуживании являются минимальными.

Операционные системы Windows

Обзор среды Microsoft Failover Cluster

Microsoft Failover Cluster Manager позволяет поместить кластерные ресурсы сервера IBM Spectrum Protect в группу кластера. Группа кластера IBM Spectrum Protect имеет сетевое имя, IP-адрес, один или несколько физических дисков, сервер DB2 и службу сервера IBM Spectrum Protect.

Сетевое имя экземпляра IBM Spectrum Protect не зависит от имени физического узла, на котором работает группа кластеров IBM Spectrum Protect. Клиенты подключаются к серверу IBM Spectrum Protect, используя сетевое имя экземпляра, а не имя узла Windows. Сетевое имя экземпляра отображается на первичный или резервный узел. Это отображение зависит от того, какому узлу принадлежит группа кластера. Клиент, использующий Windows Internet Name Service (WINS) или службы каталогов для обнаружения серверов, может автоматически отслеживать сервер IBM Spectrum Protect, когда тот перемещается между узлами. Можно автоматически отслеживать кластерный сервер без изменения или перенастройки клиента.

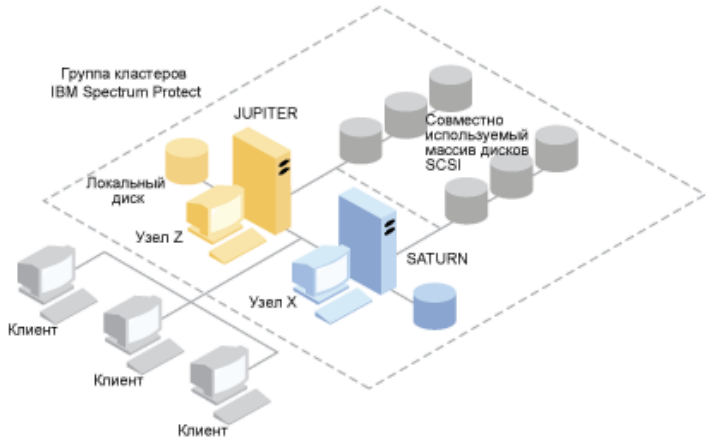
У каждой группы кластера IBM Spectrum Protect есть свой собственный диск, являющийся частью группы ресурсов кластера. Группы кластера IBM Spectrum Protect не могут между собой совместно использовать данные. У каждого сервера IBM Spectrum Protect, который сконфигурирован в группе кластера, есть своя база данных, активные журналы, журналы восстановления и набор томов пула хранения на отдельном диске. Этот диск принадлежит группе кластеров, в которой сконфигурирован сервер.

Напоминание: Microsoft Failover Cluster Manager поддерживает в качестве ресурса только IP-адрес. Поэтому любой запущенный в кластере сервер IBM Spectrum Protect должен использовать только поддерживаемый способ связи TCP/IP. Все клиенты, не использующие для связи TCP/IP, не могут получить доступ к группе кластера IBM Spectrum Protect в случае передачи управления при сбое на другой узел кластера.

В приведенном ниже примере показано, как работает виртуальный Microsoft Failover Cluster Manager для группы кластера IBM Spectrum Protect.

Допустим, что на узле Z работает кластерный сервер IBM Spectrum Protect с именем JUPITER, а на узле X - кластерный сервер IBM Spectrum Protect с именем SATURN. Клиенты соединяются с сервером IBM Spectrum Protect JUPITER и с сервером IBM Spectrum Protect SATURN, не зная, какой узел в данный момент представляет собой хост их сервера.

Рис. 1. Кластеризация с сервером JUPITER в качестве узла Z и сервером SATURN - в качестве узла X



Когда происходит сбой одного из программных или аппаратных ресурсов, выполняется обработка отказа. Ресурсы (например приложения, диски и IP-адреса) перемещаются с узла, на котором случился сбой, на один из оставшихся. Оставшийся узел:

- Принимает на себя управление группой кластера IBM Spectrum Protect
- Переводит дисковые ресурсы, сетевые ресурсы и ресурсы DB2 в оперативный режим
- Перезапускает службу IBM Spectrum Protect
- Обеспечивает доступ администраторам и клиентам

Если на узле X произойдет сбой, то узел Z примет на себя функции сервера SATURN. С точки зрения клиента это выглядит так, как если бы узел X выключился и сразу же снова включился. Все соединения клиентов с сервером SATURN прервутся, и все активные транзакции будут возвращены клиенту. После разрыва соединения клиенты должны будут заново соединиться с сервером SATURN. Положение сервера SATURN непрозрачно для клиента.

Операционные системы Windows

Отказоустойчивость ленточных устройств для узлов в кластере

Если на узле, который является хостом для группы в кластере, произойдет сбой, группу можно будет перенести на другие узлы.

Узел может быть хостом физических или логических единиц, называемых ресурсами. Администраторы организуют эти ресурсы кластера в функциональные единицы, называемые группами, и назначают группы отдельным узлам. Если в работе узла возникает сбой, сервер кластера передает группы, для которых хостом является данный узел, другим узлам кластера. Этот процесс передачи называется *обработкой отказа*. Обратный процесс, *восстановление после отказа*, выполняется, когда отказавший узел снова становится активным, и группы, переданные другим узлам, повторно передаются исходному узлу.

- Операционные системы WindowsОбработка отказов ленточных устройств, подключаемых через оптоволоконный канал
  IBM Spectrum Protect может без дополнительных аппаратных средств обрабатывать отказы ленточных накопителей, подключенных непосредственно через Fibre Channel, и библиотечных устройств для системы Microsoft Windows в кластерной среде.

Операционные системы Windows

Планирование кластерной среды

Планирование при конфигурировании в кластерной среде помогает обеспечить оптимальную производительность используемой системы. Необходимость конфигурирования системы для использования кластеров зависит от потребностей вашего предприятия.

Спланируйте конфигурацию кластера в соответствии с особенностями вашей среды. Помимо выбора правильных типов оборудования и программного обеспечения, вы должны определить порядок передачи управления при отказе.

Какие узлы кластера возьмут на себя обработку транзакций, если на узле произойдет сбой или его потребуется отключить? В двухузловом кластере планирование почти не нужно. В более сложных конфигурациях следует рассмотреть, как наилучшим образом управлять обработкой транзакций. Для обеспечения наивысшей производительности следует учитывать введение некоторой разновидности выравнивания нагрузки между узлами. Также следует гарантировать отсутствие задержек с точки зрения заказчика, а только незначительное падение производительности.

При использовании Microsoft Cluster Servers и кластеров отказоустойчивости Microsoft у каждого экземпляра сервера IBM Spectrum Protect должен быть собственный набор дисковых ресурсов. Хотя узлы могут использовать дисковые ресурсы совместно, только один узел может активно управлять диском в каждый момент времени.

Внимание: Убедитесь, что на всех компьютерах в кластере установлен один и тот же уровень Windows (Windows 2012, Windows 2012 R2 и Windows 2016).

Является ли одна конфигурация лучшей, чем другая? Чтобы определить лучшую конфигурацию, следует сравнить производительность и стоимость. Допустим, у вас имеется выделенный под сервер IBM Spectrum Protect кластер с приблизительно одинаковой производительностью узлов. Во время обработки отказа производительность конфигурации может снизиться, поскольку одному узлу придется управлять обоими экземплярами кластера IBM Spectrum Protect. Если каждый узел управляет 100 клиентами в нормальном режиме работы, то при сбое один узел должен управлять 200 клиентами.

- Операционные системы WindowsРабочая таблица конфигурирования кластера
  Запишите свои ответы на следующие вопросы планирования, прежде чем задавать конфигурацию кластера.
- Операционные системы WindowsПодготовка систем Windows для кластерной среды
  Систему Microsoft Windows можно подготовить к тому, чтобы она стала хостом для кластерной среды IBM Spectrum Protect.
- Операционные системы WindowsКонфигурирование IBM Spectrum Protect в кластере Microsoft Failover Cluster
  Процедуру конфигурирования кластера IBM Spectrum Protect надо выполнить на узлах, на которых находится группа кластера IBM Spectrum Protect.

Информация, связанная с данной:
Поддерживаемые операционные системы для IBM Spectrum Protect

Рабочая таблица конфигурирования кластера

Запишите свои ответы на следующие вопросы планирования, прежде чем задавать конфигурацию кластера.

1. Какой тип решения кластеризации лучше всего отвечает запросам вашего предприятия?
2. Какой тип шаблона обработки отказов необходим?

   Применение обработки отказов ленточных устройств также влияет на шаблон.

3. Требуется ли поддержка обработки отказов ленточных устройств?

   Проанализируйте, как ленточные устройства будут использоваться экземплярами кластера IBM Spectrum Protect. Способ использования ленточных устройств экземплярами кластера может ограничить число узлов в шаблоне переключения после отказа двумя узлами.

4. Какие ресурсы будут выделены IBM Spectrum Protect?

Тип ресурса	**Имя ресурса**
Группа ресурсов кластера	
Физические дисковые ресурсы	
IP-адрес	
Маска подсети	
Сеть	
Имя сети (имя сервера)	
Узлы	
Обработка отказов ленточных устройств (необязательно): имя устройства - оба узла	

Операционные системы Windows

Подготовка систем Windows для кластерной среды

Систему Microsoft Windows можно подготовить к тому, чтобы она стала хостом для кластерной среды IBM Spectrum Protect.

Прежде чем начать

Сделайте следующее:

1. Убедитесь, что у вас установлена служба кластера Windows.
2. Установите инструмент командной строки управления кластером, cluster.exe, который есть на установочном диске операционной системы. В системе Windows, в PowerShell, введите следующие команды:

   ```
   PS C:\> Import-Module ServerManager
   PS C:\> Add-WindowsFeature RSAT-Clustering-CmdInterface
   ```

   Другой способ: можно запустить следующие команды:

   ```
   PS C:\> Import-Module ServerManager
   PS C:\> Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
   ```

Процедура

Сделайте следующее:

1. Спланируйте размещение экземпляра сервера, базы данных, журналов и дискового хранилища на совместно используемом диске.
2. Решите, какие дисковые ресурсы будут выделены для IBM Spectrum Protect. Если вы собираетесь установить более одного сервера IBM Spectrum Protect, назначьте для каждого сервера другой набор дисков.

3. Убедитесь, что у вас есть IP-адрес и сетевое имя для каждого экземпляра сервера IBM Spectrum Protect, который вы планируете конфигурировать. Для кластера, содержащего два экземпляра кластера IBM Spectrum Protect, требуется два сетевых имени.
4. Убедитесь, что у вас есть IP-адрес и сетевое имя для кластера.
5. В менеджере кластеров Windows создайте группу ресурсов кластера и переместите в нее дисковые ресурсы. Каждому экземпляру сервера IBM Spectrum Protect необходима группа ресурсов кластера. Первоначально группа должна содержать только дисковые ресурсы. Можно переименовать существующую группу ресурсов, содержащую только дисковые ресурсы. IBM Spectrum Protect устанавливается на локальный диск каждого узла кластера.
6. Определите диск, который будет использоваться на каждом узле. Запланируйте использовать одну и ту же букву диска для каждой системы.

 Операционные системы Windows

Конфигурирование IBM Spectrum Protect в кластере Microsoft Failover Cluster

Процедуру конфигурирования кластера IBM Spectrum Protect надо выполнить на узлах, на которых находится группа кластера IBM Spectrum Protect.

Шаги этой процедуры зависят от того, конфигурирование какого узла производится. При конфигурировании основного узла в наборе создается и конфигурируется экземпляр сервера IBM Spectrum Protect. При конфигурировании остальных узлов каждый узел обновляется с использованием конкретного метода. Метод, которым обновляется узел, дает ему возможность служить хостом экземпляра сервера IBM Spectrum Protect, который создан на основном узле. Сервер IBM Spectrum Protect должен быть установлен и сконфигурирован на первом узле набора до того, как будут конфигурироваться остальные узлы набора. При нарушении этого требования конфигурирование завершится неудачно.

При конфигурировании нескольких групп кластера IBM Spectrum Protect нужно полностью сконфигурировать одну группу кластера IBM Spectrum Protect и только потом переходить к следующей. Поскольку необходимо работать с разными IP-адресами и сетевыми именами для каждой группы кластера IBM Spectrum Protect, настраивая группы кластера по отдельности, вы уменьшаете возможность ошибок.

 Операционные системы Windows

Конфигурирование IBM Spectrum Protect в кластере Microsoft Failover Cluster

Перед установкой IBM Spectrum Protect надо убедиться, что кластер правильно установлен и сконфигурирован.

Процедура

Чтобы сконфигурировать IBM Spectrum Protect в кластере восстановления после отказа Microsoft Failover Cluster, выполните следующие действия:

1. Убедитесь, что операционная система Windows установлена на всех компьютерах, являющихся частью кластера. Самую свежую информацию о поддерживаемых операционных системах Windows смотрите в техническом замечании 1243309.
2. Войдите в систему от имени ID пользователя домена. Пользователь домена должен находиться в одном домене с сервером IBM Spectrum Protect.
3. Убедитесь, что кластер отказоустойчивости установлен и сконфигурирован на всех компьютерах в кластере. Если вы собираетесь установить сервер IBM Spectrum Protect в операционной системе Windows Server 2012, то сначала установите сервер автоматизации кластера переключения после отказа и командный интерфейс кластера переключения после отказа. Чтобы установить эти компоненты, введите следующие команды из Windows 2.0 PowerShell:

   ```
   Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
   Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
   ```

4. Проверьте работоспособность каждого узла и совместно используемого диска в кластере.
5. Убедитесь в работоспособности совместно используемых ленточных устройств, если используется обработка отказов ленточных устройств IBM Spectrum Protect.

- Операционные системы WindowsПодготовка группы кластера Microsoft Failover Cluster для базового виртуального сервера
  Каждому экземпляру сервера IBM Spectrum Protect необходима группа ресурсов кластера.
- Операционные системы WindowsУстановка IBM Spectrum Protect в кластере Microsoft Failover Cluster
  Установите сервер IBM Spectrum Protect на каждом узле кластера, который является хостом кластерного сервера IBM Spectrum Protect.
- Операционные системы WindowsИнициализация сервера IBM Spectrum Protect для Microsoft Failover Cluster на основном узле
  После установки IBM Spectrum Protect на узлах в кластере нужно инициализировать сервер на основном узле.
- Операционные системы WindowsПроверка конфигурации IBM Spectrum Protect в Microsoft Failover Cluster
  Выполнив конфигурирование IBM Spectrum Protect в кластере восстановления после отказа Microsoft Failover Cluster, вы сможете просмотреть сводное окно Менеджера кластеров восстановления после отказа. Убедитесь, что кластеризация выполнена успешно и сервер IBM Spectrum Protect запущен.
- Операционные системы WindowsПроверка отказоустойчивости кластера
  По завершении конфигурирования кластера проверьте отказоустойчивость, чтобы убедиться, что узлы работают правильно.

Операционные системы Windows

Подготовка группы кластера Microsoft Failover Cluster для базового виртуального сервера

Каждому экземпляру сервера IBM Spectrum Protect необходима группа ресурсов кластера.

Прежде чем начать

Используйте для подготовки группы ресурсов программу Диспетчер отказоустойчивости кластеров на компьютере, которому принадлежит ресурс совместно используемого диска или ленточного устройства. Первоначально группа должна содержать только дисковые ресурсы. Можно создать группу и переместить в нее дисковые ресурсы. Можно также переименовать существующую группу ресурсов, содержащую только дисковые ресурсы.

При создании группы ресурсов примите во внимание следующие замечания:

- Убедитесь, что имя каждой группы ресурсов уникально. Не изменяйте имена после создания группы, поскольку это может привести к повреждению конфигурации.
- Убедитесь, что все узлы кластера подключены к сети.
- Убедитесь, что группа находится в сети и принадлежит узлу, на котором установлен исходный экземпляр сервера.

Процедура

Чтобы подготовить группу ресурсов для конфигурирования кластера, выполните следующие шаги:

1. Откройте программу Диспетчер отказоустойчивости кластеров и раскройте кластер. Щелкните правой кнопкой по Роли и щелкните по Создать пустую роль.
2. В панели Роли дважды щелкните по Новая роль и измените имя роли на понятное имя, например, TSMGROUP.
3. Щелкните правой кнопкой мыши по группе ресурсов TSMGROUP и выберите Добавить хранение.
4. В панели Добавить область хранения выберите совместно используемый том (или тома) для IBM Spectrum Protect и нажмите кнопку ОК. Появится группа ресурсов TSMGROUP, которая будет содержать добавленные вами дисковые тома.

Операционные системы Windows

Установка IBM Spectrum Protect в кластере Microsoft Failover Cluster

Установите сервер IBM Spectrum Protect на каждом узле кластера, который является хостом кластерного сервера IBM Spectrum Protect.

Процедура

Выполните для каждого узла в кластере описанные ниже шаги, чтобы установить сервер IBM Spectrum Protect:

1. Войдите в систему от имени администратора или ID пользователя домена. Пользователь домена должен входить в группу Администраторы домена.
2. Установите сервер IBM Spectrum Protect на локальном диске на каждом узле. Используйте на всех узлах одинаковую букву локального диска.
3. По завершении установки сервера перезапустите систему.

Операционные системы Windows

Инициализация сервера IBM Spectrum Protect для Microsoft Failover Cluster на основном узле

После установки IBM Spectrum Protect на узлах в кластере нужно инициализировать сервер на основном узле.

Процедура

1. Убедитесь, что все системы перезапущены после установки. Проверьте, все ли системы запустились правильно.
2. Войдите в систему от имени администратора или ID пользователя домена. Пользователь домена должен находиться в одном домене с сервером IBM Spectrum Protect.
3. Откройте программу Диспетчер отказоустойчивости кластеров и убедитесь, что ресурсы подключены и принадлежат основному узлу.
4. Начните процедуру инициализации сервера на основном узле в кластере.
5. Временно включите протокол Microsoft Windows Server Message Block (SMBv1). Следуйте инструкциям в разделе Как обнаружить, включить и отключить SMBv1, SMBv2 и SMBv3 в Windows и Windows Server. Этот шаг требуется, чтобы выполнить мастер конфигурирования IBM Spectrum Protect.
6. В меню Пуск щелкните по Все программы > Сервер IBM Spectrum Protect > Мастер по конфигурированию.
7. Следуйте указаниям мастера и нажимайте кнопку Далее. При запросе ID пользователя введите имя учетной записи домена, которая будет связана с кластером.
8. Когда инициализация завершится, нажмите кнопку Готово.
9. Отключите протокол SMBv1. Следуйте инструкциям в разделе Как обнаружить, включить и отключить SMBv1, SMBv2 и SMBv3 в Windows и Windows Server.

Операционные системы Windows

Проверка конфигурации IBM Spectrum Protect в Microsoft Failover Cluster

Выполнив конфигурирование IBM Spectrum Protect в кластере восстановления после отказа Microsoft Failover Cluster, вы сможете просмотреть сводное окно Менеджера кластеров восстановления после отказа. Убедитесь, что кластеризация выполнена успешно и сервер IBM Spectrum Protect запущен.

Процедура

Чтобы убедиться, что экземпляр сервера IBM Spectrum Protect в кластере восстановления после отказа Microsoft Failover Cluster создан и сконфигурирован правильно, выполните следующие действия:

1. В программе Диспетчер отказоустойчивости кластеров выберите экземпляр сервера. Сетевое имя, которое вы сконфигурировали, будет показано на панели Имя сервера.
2. В панели Другие ресурсы убедитесь, что показаны экземпляр сервера и ресурс сервера IBM® DB2.
3. Щелкните правой кнопкой мыши по экземпляру сервера IBM Spectrum Protect и щелкните по Перевести в оперативное состояние.

Операционные системы Windows

Проверка отказоустойчивости кластера

По завершении конфигурирования кластера проверьте отказоустойчивость, чтобы убедиться, что узлы работают правильно.

Процедура

1. Откройте Failover Cluster Manager. В разделе Другие ресурсы щелкните правой кнопкой мыши по Ресурс экземпляра(x) IBM Spectrum Protect. Щелкните по Перевести в оперативное состояние.
2. Чтобы проверить отказоустойчивость, щелкните правой кнопкой мыши по группе ресурсов кластера IBM Spectrum Protect и щелкните по Переместить.
3. Убедитесь, что передача управления со второго узла на первый узел завершилась успешно.

Операционные системы Windows

Управление кластерной средой

После настройки первоначального кластера или кластеров потребности в обслуживании являются минимальными.

Регулярно проверяйте журнал событий Windows, чтобы отслеживать деятельность узлов кластера. Используйте журнал, чтобы проверить, нет ли отказа узла и не нуждается ли он в обслуживании.

В перечисленных ниже разделах описаны ситуации, которые могут повлиять на конфигурацию или формат кластера, после того как он заработает.

- Операционные системы WindowsПеренос существующего сервера IBM Spectrum Protect в кластер
  Причина перемещения данных клиента в кластер аналогична причине добавления в кластер нового сервера. Вы хотите увеличить доступность и надежность данных для всех своих пользователей. Сервер, включаемый в состав кластера, обеспечивает дополнительный уровень защиты, гарантируя, что из-за отказавшего сервера не будут пропущены транзакции. Заданный вами порядок обработки отказов предотвратит сбои в будущем.
- Операционные системы WindowsДобавление сервера IBM Spectrum Protect с использованием резервного копирования и восстановления
  Если вы аппаратные ресурсы ограничены, то можно добавить существующий сервер IBM Spectrum Protect в кластер, используя процедуру резервного копирования и восстановления.
- Операционные системы WindowsУправление виртуальным сервером IBM Spectrum Protect в кластере
  Большинство задач по администрированию виртуального сервера IBM Spectrum Protect выполняется так же, как и в случае некластерного сервера. Для выполнения таких задач, как запуск и остановка сервера или перемещение группы ресурсов на другой узел для техобслуживания системы, необходимо использовать интерфейс Microsoft Cluster Administrator.
- Операционные системы WindowsУправление отказоустойчивостью ленточных устройств в кластере
  Регулярно проверяйте журнал событий, чтобы убедиться в правильности работы конфигурации. Если на сервере произойдет сбой, в журнал записывается ошибка. Этот журнал дает вам информацию о том, почему произошел сбой.
- Операционные системы WindowsУстранение неисправностей при помощи журнала кластера IBM Spectrum Protect
  Библиотека DLL кластерных ресурсов IBM Spectrum Protect ведет учет событий и ошибок в журнале кластера. Журнал кластера - полезное средство при устранении неполадок. Когда ведение журнала включено, в нем записываются действия каждого компонента службы кластера и результаты каждого действия.

Операционные системы Windows

Перенос существующего сервера IBM Spectrum Protect в кластер

Причина перемещения данных клиента в кластер аналогична причине добавления в кластер нового сервера. Вы хотите увеличить доступность и надежность данных для всех своих пользователей. Сервер, включаемый в состав кластера, обеспечивает дополнительный уровень защиты, гарантируя, что из-за отказавшего сервера не будут пропущены транзакции. Заданный вами порядок обработки отказов предотвратит сбои в будущем.

Об этой задаче

Чтобы перенести существующий сервер IBM Spectrum Protect в кластер, можно либо переместить клиенты, либо выполнить процедуру резервного копирования и восстановления. Способ определяется, главным образом, доступностью и мощностью других серверных компьютеров IBM Spectrum Protect в вашей системе и знакомством с процедурой резервного копирования и восстановления.

- Операционные системы WindowsПеремещение клиентов
  При перемещении клиентов с компьютера-сервера IBM Spectrum Protect, не входящего в кластер, на компьютер, входящий в кластер, вы можете постепенно переместить пользователей на новый компьютер, не прерывая работы служб. Однако оборудование должно поддерживать одновременную работу двух серверов IBM Spectrum Protect.

Задачи, связанные с данной:
Установка и обновление сервера
Операционные системы Windows

Добавление сервера IBM Spectrum Protect с использованием резервного копирования и восстановления

Если вы аппаратные ресурсы ограничены, то можно добавить существующий сервер IBM Spectrum Protect в кластер, используя процедуру резервного копирования и восстановления.

Об этой задаче

Допустим, например, что у вас нет оборудования помимо двух серверных систем, которые нужно объединить в кластер. Вы планируете использовать компьютер, на котором работает сервер IBM Spectrum Protect, в качестве узла. Выполните следующую процедуру, чтобы удалить IBM Spectrum Protect с компьютера и переустановить его в кластере:

Процедура

1. Выполните резервное копирование всех дисковых пулов хранения в пулы хранения копий.
2. Выполните резервное копирование базы данных существующего сервера IBM Spectrum Protect.
3. Выполните установку и конфигурирование кластера.
4. Восстановите базу данных на кластеризованном сервере IBM Spectrum Protect.
5. Восстановите тома дискового пула хранения из пула хранения копий.
6. После проверки наличия всех данных на кластерном сервере удалите старый сервер.

Операционные системы Windows

Управление виртуальным сервером IBM Spectrum Protect в кластере

Большинство задач по администрированию виртуального сервера IBM Spectrum Protect выполняется так же, как и в случае некластерного сервера. Для выполнения таких задач, как запуск и остановка сервера или перемещение группы ресурсов на другой узел для техобслуживания системы, необходимо использовать интерфейс Microsoft Cluster Administrator.

Об этой задаче

Интерфейс Microsoft Cluster Administrator доступен в группе программ инструментов администрирования. Этот интерфейс обеспечивает подробное представление конфигурации виртуального сервера. Конфигурация виртуального сервера включает в себя такие подробности, как физические серверы Windows, которые образуют часть кластера, их ресурсы, сетевые соединения и состояние. Просмотрите компоненты конфигурации виртуального сервера и выполните нужное действие для виртуального сервера в этом интерфейсе: запуск, остановку или восстановление после отказа. Управляйте виртуальным сервером IBM Spectrum Protect, используя интерфейс Microsoft Cluster Administrator, чтобы исключить сбои сервера и сообщения об ошибках. Например, если вы используете Windows Service Control Manager для отключения сервера, могут появиться сообщения о сбое сервера.

Вам может потребоваться переместить виртуальный сервер IBM Spectrum Protect, если сервер Windows действует как основной узел и для этого сервера требуется техобслуживание аппаратных средств или системы. Используйте интерфейс Microsoft Cluster Administrator для передачи управления виртуальным сервером IBM Spectrum Protect на дополнительный узел до завершения техобслуживания.

Операционные системы Windows

Управление отказоустойчивостью ленточных устройств в кластере

Регулярно проверяйте журнал событий, чтобы убедиться в правильности работы конфигурации. Если на сервере произойдет сбой, в журнал записывается ошибка. Этот журнал дает вам информацию о том, почему произошел сбой.

Прежде чем начать

Чтобы гарантировать, что сервер может определять или сбрасывать имена устройств после отказа, задайте для параметра SANDISCOVERY значение ON. По умолчанию для этой опции задано значение OFF. Дополнительную информацию смотрите в разделе SANDISCOVERY.

Об этой задаче

Иногда узел должен повторно присоединиться к кластеру, например:

- в случае отказа узла;
- При добавлении новой оптоволоконной платы адаптера главной шины хоста (Host Bus Adapter, HBA) (изменения оборудования)

Процедура

В любом порядке выполните следующие задачи, чтобы обеспечить успешное присоединение узла к кластеру:

- Обновите, при необходимости, накопитель и библиотеку, которые используют инструмент Кластер IBM Spectrum Protect.
- Отключите сервер IBM Spectrum Protect от сети до того, как отказавший узел повторно присоединится к кластеру. Это позволит убедиться в том, что сервер IBM Spectrum Protect, работающий на другом узле, не будет затронут.

 Операционные системы Windows

Устранение неисправностей при помощи журнала кластера IBM Spectrum Protect

Библиотека DLL кластерных ресурсов IBM Spectrum Protect ведет учет событий и ошибок в журнале кластера. Журнал кластера - полезное средство при устранении неполадок. Когда ведение журнала включено, в нем записываются действия каждого компонента службы кластера и результаты каждого действия.

Журнал кластера содержит полные сведения о работе кластера по сравнению с журналом событий Microsoft Windows. В журнале кластера записываются действия службы кластера, фиксируемые в журнале событий. В то время, как журнал событий может обозначить проблему, журнал кластера поможет разрешить эту проблему.

Журнал кластера по умолчанию разрешен в Windows. Его выходные результаты выводятся в файл журнала в папке %SystemRoot%\Cluster. Дополнительные сведения смотрите в электронной справке Windows.

Конфигурирование клиентов для приложений, виртуальных машин и компьютеров

Сервер защищает данные для клиентов, которые могут включать в себя приложения, виртуальные машины и системы. Чтобы начать защиту клиентских данных, зарегистрируйте клиентский узел на сервере и выберите расписание резервного копирования для защиты клиентских данных.

- Добавление клиентов
  После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.
- Настройка политик
  Цели организации с точки зрения защиты и хранения данных, как правило, заданы руководителями корпорации, юридическими консультантами или другими сотрудниками, выполняющими роли руководителей. *Политики* - это средство соотнести операцию IBM Spectrum Protect с целями по защите и хранению данных в вашей организации.

Добавление клиентов

После реализации решения защиты данных при помощи IBM Spectrum Protect вы можете расширить решение, добавив клиенты.

Об этой задаче

Процедура описывает базовые шаги по добавлению клиента. Более конкретные инструкции по конфигурированию клиентов смотрите в документации по продукту, который вы установили на клиентском узле. У вас могут быть следующие типы клиентских узлов:

Клиентские узлы приложений
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Системные клиентские узлы
: К системным клиентским узлам относятся рабочие станции, файл-серверы сетевого хранилища данных (NAS) и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Процедура

Чтобы добавить клиент, сделайте следующее:

1. Выберите программу, которую нужно установить на клиентском узле, и спланируйте установку. Следуйте инструкциям в Выбор программного обеспечения клиента и планирование установки.
2. Укажите, как следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в Как задать роли для резервного копирования и архивирования данных клиента.
3. Укажите, когда следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в Планирование операций резервного копирования и архивирования.
4. Чтобы позволить клиенту соединяться с сервером, зарегистрируйте клиент. Следуйте инструкциям в Регистрация клиентов.
5. Чтобы начать защищать клиентский узел, установите и сконфигурируйте выбранную программу на клиентском узле. Следуйте инструкциям в Установка и настройка клиентов.

Выбор программного обеспечения клиента и планирование установки

Для разных типов данных требуются разные типы защиты. Определите, какой тип данных вам нужно защищать, и выберите соответствующую программу.

Об этой задаче

Предпочтительная практика заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить демон приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, вы должны следовать инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Процедура

В зависимости от ваших целей выберите продукты, которые нужно установить, и ознакомьтесь с инструкциями по установке.
Совет: Если вы установите программу-клиент сейчас, вы, прежде чем сможете использовать клиент, также должны будете выполнить задачи по конфигурированию клиента, описанные в разделе Установка и настройка клиентов.

Цель	Продукт и описание	Инструкции по установке

Цель	Продукт и описание	Инструкции по установке
Защитить файл-сервер или рабочую станцию	Клиент резервного копирования и архивирования производит резервное копирование и архивирование файлов и каталогов с файл-серверов и рабочих станций в хранилище. Вы также можете восстанавливать и получать версии резервных копий и архивные копии файлов.	• Требования клиента резервного копирования и архивирования • Установить клиентов резервного копирования и архивирования UNIX и Linux • Первая установка клиента Windows
Защитить приложения с использованием резервного копирования снимков и возможностей восстановления	IBM Spectrum Protect Snapshot защищает данные с использованием интегрированного резервного копирования снимков и возможностей восстановления с учетом информации о приложениях. Вы можете защитить данные, которые хранятся в приложениях IBM программное обеспечение баз данных DB2 и SAP, Oracle, Microsoft Exchange и Microsoft SQL Server.	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
Защитить приложение электронной почты на сервере IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов IBM Domino.	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0)
Защитить приложение электронной почты на сервере Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server автоматизирует защиту данных, чтобы резервное копирование выполнялось без завершения работы серверов Microsoft Exchange.	Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Защитить базу данных IBM DB2	Интерфейс прикладного программирования (API) можно использовать для резервного копирования данных DB2 на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных IBM Informix	API клиента резервного копирования и архивирования можно использовать для резервного копирования данных Informix на сервер IBM Spectrum Protect.	Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)
Защитить базу данных Microsoft SQL	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server защищает данные Microsoft SQL.	Установка Data Protection for SQL Server в ядре сервера Windows
Защитить базу данных Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle защищает данные Oracle.	Установка Data Protection for Oracle
Защитить среду SAP	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP обеспечивает защиту, настроенную для сред SAP. Продукт предназначен для того, чтобы повышать доступность серверов базы данных SAP и сокращать рабочую нагрузку администрирования.	• Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

Цель	Продукт и описание	Инструкции по установке
Защитить виртуальную машину	IBM Spectrum Protect for Virtual Environments обеспечивает защиту, настроенную для виртуальных сред Microsoft Hyper-V и VMware. IBM Spectrum Protect for Virtual Environments можно использовать для создания постоянных инкрементных резервных копий, хранящихся на централизованном сервере, создания политик резервного копирования и восстановления виртуальных машин или отдельных файлов. Либо используйте клиент резервного копирования и архивирования, чтобы производить резервное копирование и восстановление полной виртуальной машины VMware или Microsoft Hyper-V. Можно также производить резервное копирование и восстановление файлов или каталогов с виртуальной машины VMware.	• Установка Data Protection for Microsoft Hyper-V • Установка и обновление Data Protection for VMware • Установка клиентов резервного копирования и архивирования IBM Spectrum Protect (UNIX, Linux и Windows)

Совет: Чтобы использовать клиент для управления пространством, можно установить IBM Spectrum Protect for Space Management или IBM Spectrum Protect HSM for Windows.

Как задать роли для резервного копирования и архивирования данных клиента

Прежде чем вы добавите клиент, убедитесь, что соответствующие правила определены для поддержки и архивирования клиентских данных. В ходе процесса регистрации клиента вы назначается клиентский узел в домен политики, в котором есть правила, управляющие тем, как и когда производится сохранение данных клиента.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с политиками, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Планирование операций резервного копирования и архивирования.
- Если вы не знакомы с политиками, то выполните шаги в этой процедуре.

Об этой задаче

Политики влияют на то, какой объем данных хранится в течение долгого времени и сколько времени данные сохраняются и будут доступны клиентам для восстановления. Для достижения целей для защиты данных можно обновить политику по умолчанию и создать собственные политики. Политика включает следующие правила:

- Как и когда производится резервное копирование и архивирование файлов в серверное хранилище.
- Число копий файла и время хранения копий в серверном хранилище.

В ходе процесса регистрации клиента вы назначается клиент в *домен политики*. Политика для отдельного клиента определяется правилами в домене политики, который назначен для клиента. В домене политики действующие правила находятся в активном *наборе политик*.

Когда клиент копирует или архивирует файл, файл привязывается к классу управления в активном наборе политик домена политики. *Класс управления* - это ключевой набор правил для управления данными клиента. Операции резервного копирования и архивирования на клиенте используют настройки в классе управления по умолчанию домена политики, если вы далее не настраиваете политику. Политику можно настроить, задав больше классов управления и назначив их использование через опции клиента.

Опции клиента можно задать в локальном, доступном для изменения файле в системе клиента и в наборе опций клиента на сервере. Опции в наборе опций клиента на сервере могут переопределять локальный файл опций клиента или могут добавлять в него опции.

Процедура

1. Ознакомьтесь с политиками, сконфигурированными для вашего решения - следуйте инструкциям в разделе Просмотр политик.
2. Если необходимо внести незначительные изменения для соответствия требованиям хранения данных, следуйте инструкциям в разделе Изменение политик.
3. Необязательно: Если вам нужно создать домены политики или внести расширенные изменения в политики, чтобы выполнить требования к хранению данных, смотрите раздел Настройка политик.

Просмотр политик

Просмотрите политики, чтобы определить, не нужно ли их изменить в соответствии с вашими требованиями.

Процедура

1. Чтобы просмотреть активный наборов политик для домена политики, сделайте следующее:
   a. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
   b. На странице Сводка для домена политики щелкните по вкладке Наборы политики.
   Совет: Чтобы облегчить возможность восстановления данных после атаки программы-вымогателя, следуйте инструкциям ниже:
      - Убедитесь, что значение в столбце Резервные копии - это минимум 2. Предпочтительное значение - 3, 4 или более.
      - Убедитесь, что значение в столбце Сохранять дополнительные резервные копии - это минимум 14 дней. Предпочтительное значение равно 30 или более дням.
      - Убедитесь, что значение в столбце Сохранять архивы - это минимум 30 дней.

   Если программа IBM Spectrum Protect for Space Management установлена на клиенте, то убедитесь, что создана резервная копия данных, перед тем как перемещать данные. В команде DEFINE MGMTCLASS или UPDATE MGMTCLASS задайте MIGREQUIRESBKUP=YES. Далее следуйте руководящим подсказкам.
2. Для просмотра бездействующих наборов политики для домена политики сделайте следующее:
   a. На странице Наборы политик щелкните по Конфигурировать. Теперь можно просмотреть и изменить неактивные наборы политики.
   b. Прокрутите неактивные наборы политик, используя стрелки Вперед и Назад. При просмотре неактивного набора политики параметры, которые отличают этот неактивный набор политик от активного набора политик, будут выделены.
   c. Щелкните по переключателю Конфигурировать. Теперь наборы политик больше нельзя изменять.

Изменение политик

Чтобы изменить правила, применимые к домену политики, измените активный набор политик для домена политики. Можно также активировать для домена другой набор политик.

Прежде чем начать

Изменения политики могут повлиять на хранение данных. Убедитесь, чтобы вы продолжаете резервное копирование данных, имеющих существенное значение для вашей организации, чтобы можно было восстановить эти данные, если произойдет бедствие. Также убедитесь, что в вашей системе достаточно пространства хранения для запланированных операций резервного копирования.

Об этой задаче

Вы изменяете набор политик, изменяя один или несколько классов управления в наборе политик. Если вы измените активный набор политик, изменения не будут доступны клиентам, пока вы не активируете повторно набор политик. Чтобы сделать измененный набор политик доступным клиентам, активируйте набор политик.

Хотя для домена политики можно задать несколько наборов политик, активным может быть только один набор политик. При активации другого набора политики он заменяет активный в данный момент набор политик.

Предпочтительный опыт определения политик описан в разделе Настройка политик.

Процедура

1. На странице Службы в Центр операций выберите домен политики и щелкните по Сведения.
2. На странице Сводка для домена политики щелкните по вкладке Наборы политики.

   На странице Наборы политик указано имя активного набора политики и перечислены все классы управления для этого набора политик.

3. Щелкните по переключателю Конфигурировать. Набор политик доступен для изменения.
4. Необязательно: Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
5. Измените набор политик, выполнив любое из следующих действий:

Опция	Описание
Добавьте класс управления	a. В таблице Наборы политик щелкните по +Класс управления. b. Чтобы задать правила для резервного копирования и архивирования данных, заполните поля в окне Добавить класс управления. c. Чтобы сделать класс управления классом управления по умолчанию, включите переключатель Сделать значением по умолчанию. d. Щелкните по Добавить.
Удалите класс управления	В столбце Класс управления щелкните по -. Совет: Чтобы удалить класс управления по умолчанию, нужно сначала назначить другой класс управления классом управления по умолчанию.
Сделать класс управления классом управления по умолчанию	Щелкните по радиокнопке в столбце Значение по умолчанию для класса управления. Совет: Класс управления по умолчанию управляет файлами клиента, если для файла не назначен другой класс управления или если класс управления файла не подходит для управления файлом. Чтобы убедиться в том, что клиенты всегда могут производить резервное копирование и архивирование файлов, выберите класс управления по умолчанию и для резервного копирования, и для архивирования файлов.
Изменить класс управления	Чтобы изменить свойства класса управления, обновите поля в таблице.

6. Щелкните по Сохранить.
   Внимание: При активации нового набора политик можно потерять данные. Данные, защищенные в соответствии с одним набором политик, могут оказаться незащищенными с точки зрения другого набора политик. Поэтому, прежде чем активировать набор политик, убедитесь, что разница между предыдущим набором политик и новым набором политик не вызовет потерю данных.
7. Выберите Активировать. Будет показана сводка различий между активным набором политик и новым набором политик. Убедитесь, что изменения в новом наборе политики совместимы с вашими требованиями к хранению данных; для этого выполните следующие шаги:
   a. Проверьте различия между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном наборе политик, будут связаны с классами управления с теми же именами в новом наборе политик.
   b. Укажите в активном наборе политики классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут управляться классом управления по умолчанию в новом наборе политик.
   c. Если изменения, которые должны быть реализованы набором политики, являются допустимыми, выберите переключатель Я понимаю, что эти обновления могут вызвать потерю данных и щелкните по Активировать.

Планирование операций резервного копирования и архивирования

Прежде чем зарегистрировать новый клиент на сервере, убедитесь, что существует расписание, позволяющее указать, когда выполняются операции резервного копирования и архивирования. В процессе регистрации можно назначить расписание клиенту.

Прежде чем начать

Определитесь, как продолжать:

- Если вы знакомы с расписаниями, сконфигурированными для вашего решения, и вы знаете, что они не требуют изменений, то переходите к шагу Регистрация клиентов.
- Если вы не знакомы с расписаниями или расписания нужно изменить, выполните шаги в этой процедуре.

Об этой задаче

Как правило, операции резервного копирования для всех клиентов должны выполняться ежедневно. Спланируйте рабочую нагрузку клиента и сервера, чтобы обеспечить наивысшую производительность для вашей среды хранения. Чтобы избежать перекрывания операций клиента и сервера, рассмотрите возможность запланировать выполнение операций резервного копирования и архивирования клиента по ночам. Если операции клиента и сервера будут перекрываться или для их обработки не выделят достаточно времени и ресурсов, то вы можете столкнуться со снижением производительности системы, неудачным завершением операций и другими проблемами.

Процедура

1. Проверьте доступные расписания, установив указатель мыши на Клиенты в строке меню Центр операций. Щелкните по Расписания.
2. Необязательно: Измените или создайте расписание, выполнив следующие шаги:

Опция	Описание
Изменение расписания	a. В представлении Расписания выберите расписание и щелкните по Сведения. b. На странице Сведения о расписании просмотрите сведения, щелкнув по синим стрелкам в начале строк. c. Измените параметры в расписании и нажмите на Сохранить.
Создание расписания	В представлении Расписания щелкните по +Расписание и выполните шаги по созданию расписания.

3. Необязательно: Чтобы сконфигурировать параметры расписания, которые не видны в компоненте Центр операций, используйте серверную команду. Например, вы можете счесть целесообразным запланировать операцию клиента, которая создает резервную копию определенного каталога и назначает для него класс управления, отличающийся от класса управления по умолчанию.
   a. На странице Обзор в компоненте Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
   b. Введите команду DEFINE SCHEDULE, чтобы создать расписание, или команду UPDATE SCHEDULE, чтобы изменить расписание. Дополнительные сведения о командах смотрите в разделах DEFINE SCHEDULE (определение расписания выполнения административных команд) или UPDATE SCHEDULE (Изменить запланированное задание клиента).

Задачи, связанные с данной:
Настройка расписания для ежедневных операций

Регистрация клиентов

Зарегистрируйте клиент, чтобы убедиться, что он может соединиться с сервером, а сервер может защитить данные клиента.

Прежде чем начать

Узнайте, нужен ли клиенту ID администратора с правами владельца клиента в клиентском узле. Чтобы узнать, каким клиентам требуется ID администратора, смотрите публикацию technote 7048963.
Ограничение: Для клиентов некоторых типов требуется совпадение имени клиентского узла и ID администратора. Этих клиентов невозможно аутентифицировать с помощью метода Lightweight Directory Access Protocol (LDAP), внедренного в версии 7.1.7. Подробную информацию об этом методе аутентификации, который иногда называется интегрированным режимом, смотрите в документе Аутентификация пользователей с использованием базы данных Active Directory.

Процедура

Чтобы зарегистрировать клиент, выполните одно из следующих действий:

- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью команды REGISTER NODE и задайте параметр USERID:

  ```
  register node имя_узла пароль userid=имя_узла
  ```

  где *имя_узла* - это имя узла и *пароль* - это пароль узла. Дополнительные сведения смотрите в разделе Регистрация узла.
- Если клиенту требуется ID администратора, то зарегистрируйте клиент с помощью мастера добавления клиента Центр операций. Сделайте следующее:
  a. В панели меню Центра операций выберите Клиенты.
  b. В таблице Клиенты щелкните по + Клиент.
  c. Выполните шаги в мастере Добавить клиент:
     i. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель Включить в области Дедупликация данных на стороне клиента.
     ii. В окне Конфигурация скопируйте значения TCPSERVERADDRESS, TCPPORT, NODENAME, и DEDUPLICATION.
     Совет: Запишите значения опций и сохраните их в надежном месте. По завершении регистрации клиента и установки программы на клиентском узле используйте значения для конфигурирования клиента.
     iii. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     iv. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     v. Щелкните по Добавить клиент.

Ссылки, связанные с данной:
DECOMMISSION NODE (Списать клиентский узел)
DECOMMISSION VM (Списать виртуальную машину)
QUERY NODE (Запросить информацию об узлах)
REMOVE REPLNODE (Удалить клиентский узел из репликации)

Установка и настройка клиентов

Чтобы начать защищать клиентский узел, нужно установить и сконфигурировать выбранную программу.

Процедура

Если вы уже установили программу, начните с шага 2.

1. Выполните одно из следующих действий.
   - Чтобы установить программу в приложении или на клиентском узле, выполните инструкции.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows Совет: Можно также обновить существующие клиенты при помощи Центр операций. Инструкции смотрите в разделе Планирование обновлений клиента.
IBM Spectrum Protect for Databases	▪ Установка Data Protection for Oracle ▪ Установка Data Protection for SQL Server в ядре сервера Windows
IBM Spectrum Protect for Mail	▪ Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) ▪ Установка Data Protection for IBM Domino в системе Windows (V7.1.0) ▪ Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Программа	Ссылка на инструкции
IBM Spectrum Protect Snapshot	▪ Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux ▪ Установка и обновление IBM Spectrum Protect Snapshot для VMware ▪ Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Enterprise Resource Planning	▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 ▪ Установка IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- Чтобы установить программу на клиентском узле виртуальной машины, выполните инструкции для выбранного типа резервного копирования.

Тип резервного копирования	Ссылка на инструкции
Если вы собираетесь создавать полные резервные копии VMware виртуальных машин, установите и сконфигурируйте клиент резервного копирования и архивирования IBM Spectrum Protect.	▪ Установить клиентов резервного копирования и архивирования UNIX и Linux ▪ Первая установка клиента Windows
Если вы собираетесь установить постоянные полные резервные копии виртуальных машин, установите и сконфигурируйте IBM Spectrum Protect for Virtual Environments и клиент резервного копирования и архивирования на одном и том же клиентском узле или на разных клиентских узлах.	▪ Электронная документация по продукту IBM Spectrum Protect for Virtual Environments Совет: Программу для IBM Spectrum Protect for Virtual Environments и для клиента резервного копирования и архивирования можно получить в пакете установки IBM Spectrum Protect for Virtual Environments.

2. Чтобы разрешить клиенту соединяться с сервером, добавьте или обновите значения опций TCPSERVERADDRESS, TCPPORT и NODENAME в файле опций клиента. Используйте значения, записанные вами при регистрации клиента (раздел Регистрация клиентов).
   - Если клиенты установлены в операционной системе AIX, Linux, Mac OS X или Oracle Solaris, добавьте значения в файл системных опций клиента, dsm.sys.
   - Если клиенты установлены в операционной системе Windows, добавьте значения в файл dsm.opt.

   По умолчанию, файлы опций находятся в каталоге установки.
3. Если вы установили клиент резервного копирования и архивирования в операционной системе Linux или Windows, то установите служба управления клиентами на клиенте. Выполните инструкции в разделе Сбор диагностической информации с использованием служб управления клиентом.
4. Сконфигурируйте клиент для выполнения запланированных операций. Следуйте инструкциям в Конфигурирование клиента для выполнения запланированных операций.
5. Необязательно: Сконфигурируйте связь через брандмауэр. Следуйте инструкциям в Конфигурирование взаимодействий между клиентом и сервером через брандмауэр.
6. Запустите тестовое резервное копирование, чтобы проверить, защищены ли данные, как вы планировали. Например, для клиента резервного копирования и архивирования выполните следующие шаги:
   a. Выберите на странице Клиенты компонента Центр операций клиент, для которого вы хотите выполнить резервное копирование, и щелкните по Резервное копирование.
   b. Убедитесь, что резервное копирование выполнено успешно и что нет ни предупреждений, ни сообщений об ошибках.
7. Следите за результатами запланированных операций клиента в компоненте Центр операций.

Дальнейшие действия

Если требуется изменить набор объектов для резервного копирования, выполните инструкции в разделе Изменение объема резервного копирования клиента.

Конфигурирование клиента для выполнения запланированных операций

Вы должны сконфигурировать и запустить планировщик клиента на клиентском узле. Планировщик клиента обеспечивает взаимодействие между клиентом и сервером, чтобы могли выполняться запланированные операции. Например, запланированные операции обычно включают в себя резервное копирование файлов с клиента.

Об этой задаче

Предпочтительный метод заключается в том, чтобы установить клиент резервного копирования и архивирования на всех клиентских узлах - тогда вы сможете сконфигурировать и запустить приемник клиента на клиентском узле. Приемник клиента разработан для эффективного выполнения запланированных операций. Приемник клиента управляет планировщиком клиента, чтобы планировщик запускался, только когда это требуется:

- Когда наступило время запросить сервер о следующей запланированной операции
- Когда наступило время запустить следующую запланированную операцию

Используя приемник клиента, вы можете сократить число фоновых процессов на клиенте и помочь избежать проблем сохранения памяти.

Приемник клиента выполняет расписания для следующих продуктов: клиент резервного копирования и архивирования, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail и IBM Spectrum Protect for Virtual Environments. При установке продукта, для которого приемник клиента не выполняет расписания, следуйте инструкциям по конфигурированию в документации по продукту, чтобы можно было выполнять запланированные операции.

Если на вашем предприятии используется сторонний инструмент планирования в качестве стандартной практики, можно использовать этот инструмент планирования как альтернативу приемнику клиентов. Как правило, сторонние инструменты планирования запускают программы-клиенты напрямую, используя команды операционной системы. Чтобы сконфигурировать сторонний инструмент планирования, смотрите документацию по продукту.

Процедура

Чтобы сконфигурировать и запустить планировщик клиента с использованием приемника клиента, следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.
c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

f. Запустите приемник клиента, введя в командной строке следующую команду:

```
/usr/bin/dsmcad
```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте в файл запуска системы (обычно, /etc/inittab) следующую запись:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Демон Client Acceptor
```

Linux

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Щелкните по вкладке Веб-клиент.

c. В поле Опции управляемых служб щелкните по Расписание. Если вы также хотите, чтобы приемник клиента управлял веб-клиентом, щелкните по опции И то, и другое.
d. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции passwordaccess в файле dsm.sys значение `generate`.
e. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

```
dsmc query sess
```

f. Запустите приемник клиента, войдя в систему от имени ID пользователя root и введя следующую команду:

```
service dsmcad start
```

g. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте службу, введя в командной строке оболочки следующую команду:

```
# chkconfig --add dsmcad
```

MAC OS X

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Изменить > Предпочтения клиента.
b. Чтобы планировщик мог запускаться без участия оператора, щелкните по Авторизация, выберите Генерирование пароляи щелкните по Применить.
c. Чтобы указать, как осуществляется управление службами, щелкните по Веб-клиент, выберите Расписание, щелкните по Применить и выберите OK.
d. Чтобы сгенерированный пароль был сохранен, перезапустите клиент резервного копирования и архивирования.
e. Используйте для запуска приемника клиента приложение Инструменты IBM Spectrum Protect для администраторов.

Windows

a. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите Утилиты > Мастер настройки > Помочь мне сконфигурировать Планировщик клиента. Щелкните по Далее.
b. Прочтите информации на странице мастера планировщика и нажмите Далее.
c. На странице Задача планировщика выберите Установить новый или дополнительный планировщик и нажмите Далее.
d. На странице Имя и расположение планировщика задайте имя для добавляемого планировщика клиента. Затем выберите Использовать Client Acceptor Daemon (CAD), чтобы управлять планировщиком, и нажмите Далее.
e. Введите имя, которое вы хотите присвоить этому приемнику клиента. Имя по умолчанию - Client Acceptor. Щелкните по Далее.
f. Выполните конфигурирование, выполняя шаги в мастере.
g. Обновите файл опций клиента, dsm.opt, и задайте для опции passwordaccess значение generate.
h. Чтобы сохранить пароль клиентского узла, введите в командной строке следующую команду:

```
dsmc query sess
```

Когда вам это предложат, введите пароль клиентского узла.
i. Запустите службу приемника клиента из панели Управление службами. Например, если вы использовали имя по умолчанию, запустите Служба Client Acceptor. Не запускайте службу планировщика, заданную вами на странице Имя и местонахождение планировщика. Служба планировщика автоматически запускается и останавливается службой приемника клиента по мере необходимости.

Конфигурирование взаимодействий между клиентом и сервером через брандмауэр

Если клиент должен связываться с сервером через брандмауэр, нужно включить связь между клиентом и сервером через брандмауэр.

Прежде чем начать

Если для регистрации клиентов вы использовали мастер добавления клиентов, найдите в файле опций клиента значения опций, полученные вами в ходе этого процесса. Для указания портов можно использовать значения.

Об этой задаче

Внимание: Не конфигурируйте брандмауэр, используя метод, который мог бы вызвать прекращение сеансов, используемых сервером или агентом хранения. Прекращение действительного сеанса может вызвать непредсказуемые последствия. Может показаться, что процессы и сеансы остановились из-за ошибок ввода-вывода. Чтобы помочь исключить сеансы из ограничений тайм-аута, сконфигурируйте известные порты для компонентов IBM Spectrum Protect. Убедитесь что для серверной опции KEEPALIVE осталось заданным значение по умолчанию YES. Это поможет вам убедиться, что связи клиент/сервер не прерывается. Инструкции относительно того, как задать опцию сервера KEEPALIVE смотрите в разделе KEEPALIVE.

Процедура

Откройте следующие порты, чтобы разрешить доступ через брандмауэр:

Порт TCP/IP для клиента резервного копирования и архивирования, административного клиента командной строки и планировщика клиента
: Задайте порт, используя опцию tcpport в файле опций клиента. Опция tcpport в файле опций клиента должна совпадать с опцией TCPPORT в файле опций сервера. Значение по умолчанию - 1500. Если вы решите использовать какое-либо значение, отличающееся от значения по умолчанию, задайте число в диапазоне 1024-32767.

Порт HTTP для включения взаимодействий между веб-клиентом и удаленными рабочими станциями
: Задайте порт для удаленной рабочей станции, задав опцию httpport в файле опций клиента удаленной рабочей станции. Значение по умолчанию - 1581.

Порты TCP/IP для удаленной рабочей станции
: Значение по умолчанию равно 0 (ноль); оно указывает, что два свободных номера портов случайным образом назначаются удаленной рабочей станции. Если вы не хотите, чтобы номера портов назначались произвольным образом, задайте значения, задав опцию webports в файле опций клиента удаленной рабочей станции.

Порт TCP/IP для сеансов администрирования
: Задайте порт, на котором сервер ожидает требований установления сеансов административного клиента. Значение опции клиента tcpadminport должно совпадать с опцией сервера TCPADMINPORT. Таким способом вы сможете защитить административные сеансы в частной сети.

Планирование обновлений клиента

Запланируйте автоматическую установку обновлений ПО для клиентов резервного копирования-архивирования IBM Spectrum Protect. Эта функция иногда называется *внедрение клиента*.

Прежде чем начать

Для планирования обновлений клиентов при помощи Центра операций надо сконфигурировать среду для соответствия следующим требованиям:

Требования к серверу
: Серверы IBM Spectrum Protect должны соответствовать следующим требованиям:

- IBM Spectrum Protect V8.1.3 или новее надо установить на хаб-сервере и подчиненных серверах.
- Для хаб-сервера и подчиненных серверов надо указать адрес высокого уровня и адрес низкого уровня. Можно сконфигурировать эти настройки при помощи команд SET SERVERHLADDRESS и SET SERVERLLADDRESS.
- Надо задать пароль сервера на хаб-сервере. Можно сконфигурировать этот параметр при помощи команды SET SERVERPASSWORD.
- Хаб-сервер должен быть определен на подчиненных серверах. Это определение не выполняется автоматически, когда подчиненные серверы добавляются к Центру операций. Чтобы задать сервер хаба, введите команду DEFINE SERVER и используйте вторую опцию в синтаксисе в документации команды. Например, введите следующую команду на каждом подчиненном сервере:

```
DEFINE SERVER имя_хаба SERVERPASSWORD=пароль_хаба HLA=IP_хаба
LLA=порт_хаба SSL=NO SESSIONSECURITY=TRANSITIONAL
```

где переменные соответствуют следующим параметрам хаб-сервера: *имя_хаба* - это имя сервера, *пароль_хаба* - это пароль сервера, *ip_хаба* - это высокоуровневый адрес, а *порт_хаба* - это низкоуровневый адрес.
- Порт, заданный опцией сервера RESTHTTPSPORT, должен быть открыт, чтобы разрешить защищенные взаимодействия между центром операций и хаб-сервером. Номер порта по умолчанию - 8443.
- У подчиненных серверов должен быть пул хранения каталога-контейнера или пул хранения FILE, доступный для хранения пакетов обновления. Центр операций автоматически выбирает пул хранения для использования.

Требования к клиентам

Клиенты резервного копирования-архивирования IBM Spectrum Protect, которые вы планируете обновлять при помощи Центра операций, должны отвечать следующим требованиям:

- Для опции passwordaccess должно быть задано значение generate.
- Для опции клиента autodeploy нужно задать значение, отличающееся от no. Более подробную информацию об этой опции смотрите в разделе Автоматическое внедрение.
- Тридцатидвухразрядные клиенты резервного копирования-архивирования не поддерживаются. Если 32-разрядный клиент резервного копирования-архивирования обнаружен в 64-разрядной операционной системе, клиент будет обновлен до 64-разрядной версии.
- Планировщик клиента должен работать.
- Система клиента должна работать, а клиент, должен быть соединен с сервером IBM Spectrum Protect хотя бы один раз.

Клиенты Microsoft Windows должны отвечать следующим дополнительным требованиям:

- Планировщик клиента должен быть запущен как служба Windows, а не из командной строки. Для уменьшения шанса перезапуска служба планировщика закрывается, прежде чем новый клиент будет установлен и перезапущен после установки. Если планировщик не работает как служба Windows, то для обновления клиента требуется перезапуск.
- Требуется версия утилиты реестра Windows (reg.exe) для командной строки. Этот инструмент обычно устанавливается как часть установки операционной системы на поддерживаемых операционных системах Windows.

Об этой задаче

Центр операций можно использовать для одновременного обновления нескольких клиентов в запланированное время.

Пакеты обновления автоматически скачиваются на сервер хаба, импортируются и реплицируются на подчиненные серверы. Когда запускается расписание обновления, файлы из пакета установки копируются в систему клиента и клиент обновляется до указанной версии программы.

ограничения:

- Спланировать можно обновления только клиента резервного копирования-архивирования. Обновления для других типов клиентов надо будет устанавливать вручную.
- Программу клиента резервного копирования-архивирования нельзя обновить, используя другие менеджеры внедрения IBM Spectrum Protect одновременно.
- Кластерная среда служб Microsoft Windows не поддерживается.
- Не планируйте автоматическое внедрение клиентов в системах, в которых установлены любые из следующих приложений:
  - IBM Spectrum Protect for Virtual Environments
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Enterprise Resource Planning
- Чтобы управлять обновлениями, центр операций создает объекты политики, включая классы устройств, пулы хранения и домены, на хаб-сервере и на подчиненных серверах. Для этих объектов используется следующий порядок именования: `IBM_DEPLOY_CLIENTS`. Чтобы не мешать операциям обновления, не изменяйте эти объекты.
- Если вы вручную сконфигурировали внедрение клиента для более ранней версии сервера, нужно удалить объекты политики, заданные вами допланирования обновлений клиентов с использованием центра операций.
- Можно запланировать обновления только для существующих клиентов. Центр операций невозможно использовать для установки нового клиента.

Информацию об установке ПО клиента резервного копирования-архивирования вручную смотрите в разделе Установка клиента резервного копирования-архивирования IBM Spectrum Protect в документации по IBM Spectrum Protect.

Информацию об установке других клиентов IBM Spectrum Protect смотрите в разделе Комплекты продуктов и связанные продукты.

Процедура

1. В строке меню Центра операций щелкните по Обновления > Клиенты. Откроется страница Обновления клиента резервного копирования-архивирования.
2. Используйте информацию на странице, чтобы понять, который выпуск установить, щелкните по Планировать обновление и выполните шаги в мастере.

Дальнейшие действия

Чтобы отследить, отменить или перенести обновления, щелкните по Обновления > Запланировано.

Чтобы диагностировать и решать проблемы, смотрите технические замечания technote 2007749.

Информация, связанная с данной:
SET SERVERHLADDRESS (установка высокоуровневого адреса сервера)
SET SERVERLLADDRESS (установка низкоуровневого адреса сервера))
SET SERVERPASSWORD (установка серверного пароля)
DEFINE SERVER (Задать сервер для обмена данными между серверами)
RESTHTTPSPORT

Настройка политик

Цели организации с точки зрения защиты и хранения данных, как правило, заданы руководителями корпорации, юридическими консультантами или другими сотрудниками, выполняющими роли руководителей. *Политики* - это средство соотнести операцию IBM Spectrum Protect с целями по защите и хранению данных в вашей организации.

Об этой задаче

Чтобы автоматически управлять защитой и хранением данных, вы задаете политики, которые представляют собой правила, заданные вами на сервере. Политики влияют на то, какой объем данных хранится в течение долгого времени и сколько времени данные сохраняются и будут доступны клиентам для восстановления. Настройте политики, чтобы они соответствовали целям защиты данных в вашей организации.

Вы выбираете политику, управляющую данными клиента, назначая клиент в домен политики. У клиентов разных типов разные требования к хранению, и, как правило, требуется настраивать и создавать правила политики.

При установке сервера у него, по умолчанию, есть одна политика в одном домене политики. Вы можете настроить эту политику и можете создать свою собственную политику.

- Основные понятия, связанные с политикой
  Политика для определенного клиента определяется параметрами в домене политики, в который добавлен клиент.
- Настройка политики
  Вы можете настроить существующие политики, так чтобы они соответствовали новым или измененным требованиям к хранению данных в вашей организации. Изменение домена политики или копирование существующего домена политики - это стандартный способ начать настройку политики.
- Создание политики путем копирования существующей политики
  Вы можете создавать политики, копируя существующие политики, а затем изменяя части, которые вы хотите изменить.
- Создание домена политики
  Вам может потребоваться создать новый домен политики для каждого типа клиента, защищенного сервером. Вам также может понадобиться разделить обязанности для клиентов среди нескольких администраторов, предоставив им полномочия на доступ к определенным доменам политики.
- Управление операциями клиента через наборы опций клиентов
  Наборы опций клиентов можно использовать, чтобы централизованно управлять опциями обработки, используемых клиентами для таких операций, как резервное копирование. Наборы опций клиентов помогают убедиться, что данные непротиворечивым образом защищены в соответствии с вашими требованиями. Набор опций клиента может переопределить опции в локальном файле опций клиента и может добавить опции, которых нет в локальном файле опций клиента.

Основные понятия, связанные с политикой

Политика для определенного клиента определяется параметрами в домене политики, в который добавлен клиент.

В ходе процесса регистрации клиента вы назначается клиент в *домен политики*. Политика для каждого клиента определяется правилами в домене политики, который назначен для клиента. В домене политики действующие правила находятся в активном *наборе политик*.

Когда клиент копирует или архивирует файл, файл привязывается к классу управления в активном наборе политик домена политики. *Класс управления* - это ключевой набор правил для управления данными клиента. Операции резервного копирования и архивирования на клиенте используют параметры в классе управления по умолчанию для домена политики, если вы не настроите политику.

Политику можно настроить, задав больше классов управления в наборе политик, активировав набор политики и назначив использование новых классов управления через опции клиента.

Опции клиента можно задать в локальном, доступном для изменения файле в системе клиента и в наборе опций клиента на сервере. Опции в наборе опций клиента на сервере могут переопределять локальный файл опций клиента или могут добавлять в него опции.

Сервер использует политику в классах управления, чтобы управлять файлами на основе того, являются ли версии файлов активными или неактивными. Самая последняя резервная или архивная копия файла является *активной версией*. Активные версии никогда не удаляются из серверного хранилища.

Версии резервных копий, кроме самой последней версии, называются *неактивными версиями*. Активная версия файла становится неактивной, когда происходит одно из следующих событий:

- Снова создается резервная копия файла, из-за чего в серверном хранилище образуется более поздняя версия файла.
- Файл удаляется из хранилища на клиентском узле, а затем запускается операция инкрементного резервного копирования. *Инкрементное резервное копирование* - это стандартная операция резервного копирования для клиента, которая создает резервные копии только тех файлов, которые изменились после последней операции резервного копирования.

Параметры в классе управления, связанные с файлом, определяют, как долго сохраняются неактивные версии файла и сколько будет этих версий.

При *обработке устаревания* применяются правила политики, указывающие, когда неактивные версии становятся больше не нужны, то есть, когда истекает срок хранения версий. В процессе обработки устаревших данных на сервере применяются правила политики, заданные вами для хранения данных, и вы должны убедиться, что вы запланировали регулярную обработку устаревания. Например, если текущая политика предусматривает хранение только четырех версий файла, то пятая, самая ранняя, будет считаться устаревшей. При проверке срока устаревания сервер удаляет из базы данных записи об устаревших версиях; при этом сами версии фактически удаляются из серверного хранилища.

- Хранение версий резервных копий и окончание их действия
  Несколько версий резервных копий файлов важны, так как пользователи могут постоянно обновлять файлы и им может потребоваться восстановить файл на другие моменты времени. Параметры политики управляют тем, какие версии резервных копий сервер оставляет в серверном хранилище, и они влияют на то, что смогут восстановить пользователи.
- Активация политики после обновления
  При внесении обновлений в политику обновления не вступают в силу, пока вы не активируете обновленный набор политик.

Информация, связанная с данной:
Полное и частичное инкрементное резервное копирование

Хранение версий резервных копий и окончание их действия

Несколько версий резервных копий файлов важны, так как пользователи могут постоянно обновлять файлы и им может потребоваться восстановить файл на другие моменты времени. Параметры политики управляют тем, какие версии резервных копий сервер оставляет в серверном хранилище, и они влияют на то, что смогут восстановить пользователи.

Вы можете задать версии, которые сервер будет хранить в серверном хранилище, используя параметры в классе управления:

- Задайте срок в днях, в течение которого следует хранить версии резервных копий.
  Вы задаете срок в днях, в течение которого следует хранить версии резервных копий, с помощью параметров в компоненте Центр операций:
  - Параметр Оставить лишние резервные копии, указывающий, в течение скольких дней следует хранить неактивные версии резервных копий. Дни отсчитываются, начиная со дня, когда версия стала неактивной.

    Если вы используете команды, введите команду DEFINE COPYGROUP с параметром RETEXTRA.

    Совет: Чтобы помочь вам убедиться, что файлы можно будет восстановить после инцидента с вредоносной программой, например, атакой программы, требующей выкупа, задайте значение, равное хотя бы 14 дням. Предпочтительное значение равно 30 или более дням.
  - Параметр Оставить удаленные резервные копии, который указывает, в течение сколиких дней следует хранить последнюю версию резервной копии файла, который был удален из клиентской файловой системы.

    Если вы используете команды, введите команду DEFINE COPYGROUP с параметром RETONLY.

    Совет: Чтобы помочь вам убедиться, что файлы можно будет восстановить после инцидента с вредоносной программой, например, атакой программы, требующей выкупа, задайте значение, равное хотя бы 30 дням.
- Задайте число версий, которые следует хранить.
  Вы задаете число версий резервных копий с помощью параметров в компоненте Центр операций:
  - Параметр Резервные копии, который представляет собой число версий, которые следует хранить, если файл все еще существует в файловой системе клиента.

    Если вы используете команды, введите команду DEFINE COPYGROUP с параметром VEREXISTS.

    Совет: Чтобы помочь вам убедиться, что файлы можно будет восстановить после инцидента с вредоносной программой, например, атакой программы, требующей выкупа, задайте значение, равное хотя бы 2. Предпочтительные значения: 3, 4 или больше.
  - Параметр Удаленные резервные копии, который представляет собой число версий, которые следует хранить, если файл удаляется из файловой системы клиента.

    Если вы используете команды, введите команду DEFINE COPYGROUP с параметром VERDELETED.

- Задайте комбинацию числа версий и срока в днях, в течение которого их следует хранить.
  Параметры взаимодействуют друг с другом, определяя версии резервных копий, которые хранятся на сервере. Убедитесь, чтобы вы поняли, какие параметры являются более приоритетными и какие взаимодействия могут происходить:
  - Если число неактивных резервных версий превысит число, заданное параметрами Резервные копии и Удаленные резервные копии, самая первая версия устареет, и сервер удалит файл из базы данных во время следующей обработки устаревания.
  - На на число неактивных версий, хранимых на сервере, также влияет параметр Оставить лишние резервные копии. Неактивные версии устаревают, когда число дней, в течение которых они были неактивны, превышает значение, указанное для хранения дополнительных версий, даже если количество версий не превышено.

- Истечение срока хранения файлов и обработка таких файлов
  Срок хранения файлов истекает, когда для них будут превышены критерии хранения, заданные в политике. Обработка устаревания на сервере удаляет файлы с истекшим сроком хранения из базы данных сервера, а файлы удаляются из серверного хранилища.
- Пример: Хранение данных, когда в политике используется только управление на основе времени
  Самый простой способ управлять хранением данных заключается в том, чтобы использовать только управление политикой на основе времени. Когда управление политикой осуществляется только на основе времени, версии файлов хранятся в течение определенного числа дней с того момента, как версии становятся неактивными.
- Пример: Хранение данных, когда в политике используется и управление на основе версий, и управление на основе времени
  Использование в политике и управления на основе версий, и управления на основе времени, позволяет обеспечить высокую гибкость при управлении хранением данных, но также повышает сложность. Чтобы понять взаимодействия между способами управления, ознакомьтесь с примерами политики и их влиянием на хранение версий резервных копий одного файла в течение одного месяца.
- Взаимодействия между параметрами политики
  Параметры политики на основе времени и на основе версий взаимодействуют при совместном использовании в

классе управления для политики. Частота резервного копирования клиента также влияет на версии резервных копий, которые хранятся для клиента.

Истечение срока хранения файлов и обработка таких файлов

Срок хранения файлов истекает, когда для них будут превышены критерии хранения, заданные в политике. Обработка устаревания на сервере удаляет файлы с истекшим сроком хранения из базы данных сервера, а файлы удаляются из серверного хранилища.

Срок хранения файлов истекает при следующих условиях:

- При удалении пользователями файловых пространств с клиентских узлов
- Пользователи отмечают файлы, как устаревшие, используя команду EXPIRE на клиенте
- Для версии резервной копии файла оказались превышены критерии хранения резервных копий (срок хранения файла и число сохраняемых неактивных версий файла)
- Для архивного файла оказался превышен критерий времени для архивных файлов (срок хранения архивных копий)
- Если срок хранения набора резервных копий превышает срок, заданный для набора резервных копий

Сервер удаляет файлы с истекшим сроком хранения из своей базы данных только в процессе проверки срока хранения файлов. После удаления таких файлов из базы данных сервер может повторно использовать место в пулах хранения, которое они занимали. Убедитесь, что периодически выполняется процедура обработки файлов с истекшим сроком хранения, чтобы сервер мог повторно использовать освободившееся пространство.

Ограничения при обработке устаревания

Использование некоторых функций влияет на обработку устаревания.

Репликация
: Если вы используете несходные политики на исходном сервере и на сервере назначения, файлы, помеченные для немедленного устаревания на сервере репликации источника не удаляются, пока они не будут реплицированы на сервер репликации назначения. Если вы не используете несходные политики, файлы, помеченные для немедленного устаревания на сервере репликации источника удаляются немедленно.

  Для сервера репликации назначения, если файлы помечены как файлы с истекшим сроком действия, они удаляются, когда сервер назначения репликации выполняет обработку устаревания.

Хранение архивных данных на основе событий
: Срок хранения архивного файла не может истечь, если для него задана задержка удаления. Если для файла не задана задержка, то он обрабатывается в соответствии с существующей процедурой устаревания.

Информация, связанная с данной:
Хранение и высвобождение устаревания/удаления

Пример: Хранение данных, когда в политике используется только управление на основе времени

Самый простой способ управлять хранением данных заключается в том, чтобы использовать только управление политикой на основе времени. Когда управление политикой осуществляется только на основе времени, версии файлов хранятся в течение определенного числа дней с того момента, как версии становятся неактивными.

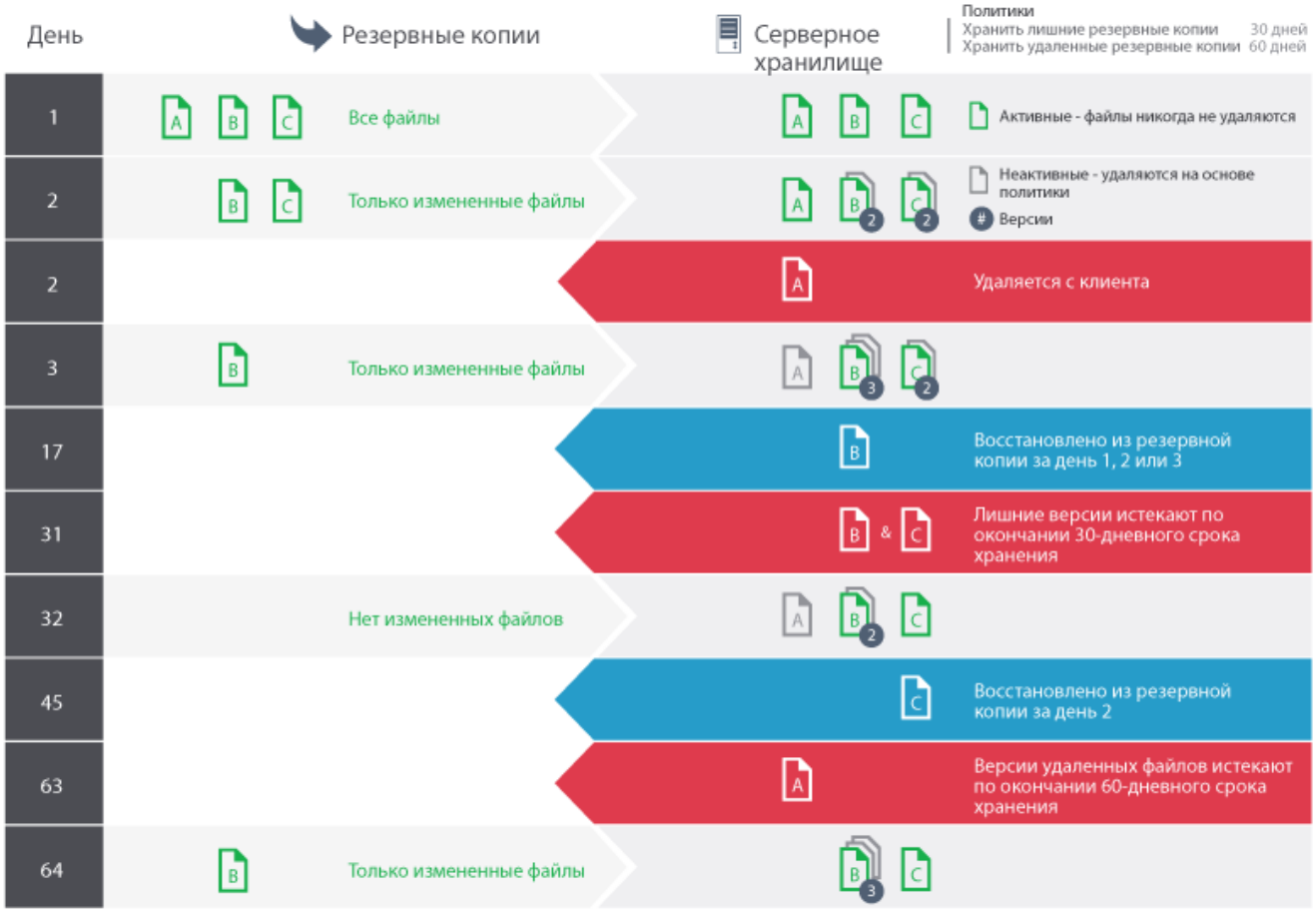
В случае политики, основанной только на времени, вы используете элементы управления Оставить лишние резервные копии и Оставить удаленные резервные копии. Этот тип политики не ограничивает число версий файлов. Если клиенты часто производят резервное копирование, убедитесь, что серверное хранилище сможет обработать потенциальное число версий файлов.

На приведенном ниже рисунке показано, как файлы с клиента обрабатываются сервером с течением времени, по мере того, как клиент выполняет ежедневную операцию инкрементного резервного копирования.

В этом примере у политики есть следующие характеристики:

- Последняя версия файла сохраняется всегда, при условии, что файл все еще существует в клиентской системе. Последняя версия является активной версией. Эта характеристика является частью каждой политики на сервере.

- Параметру Оставить лишние резервные копии присваивается значение, равное 30 дням. После создания более поздней резервной копии версия файла становится неактивной и хранится в серверном хранилище в течение 30 дней.
- Параметру Оставить удаленные резервные копии присваивается значение, равное 60 дням. После удаления файла клиентской системы все версии файла в серверном хранилище становятся неактивными. Эти неактивные версии хранятся в течение 60 дней, после того как версии файла станут неактивными.



Пример: Хранение данных, когда в политике используется и управление на основе версий, и управление на основе времени

Использование в политике и управления на основе версий, и управления на основе времени, позволяет обеспечить высокую гибкость при управлении хранением данных, но также повышает сложность. Чтобы понять взаимодействия между способами управления, ознакомьтесь с примерами политики и их влиянием на хранение версий резервных копий одного файла в течение одного месяца.

Смотрите разделы Табл. 1 и Рис. 1. Клиент производит резервное копирование файла REPORT.TXT четыре раза за один месяц, с 23 марта по 23 апреля. Параметры в группе резервных копий класса управления, с которым связан файл REPORT.TXT, определяют способ обработки этих резервных версий сервером. В Табл. 2 показано, как разные параметры групп копий могут повлиять на версии по состоянию на 24 апреля (один день после последнего резервного копирования файла).

Табл. 1. Состояние версий резервных копий REPORT.TXT на 24 апреля

Версия	**Дата создания**	**Число дней с того момента, как версия стала неактивной**
Активно	23 апреля	(нет данных)
Неактивная 1	13 апреля	1 (с 23 апреля)
Неактивная 2	31 марта	11 (с 13 апреля)

Версия	Дата создания	Число дней с того момента, как версия стала неактивной
Неактивная 3	23 марта	24 (с 31 марта)

Рис. 1. Активные и неактивные версии файла REPORT.TXT

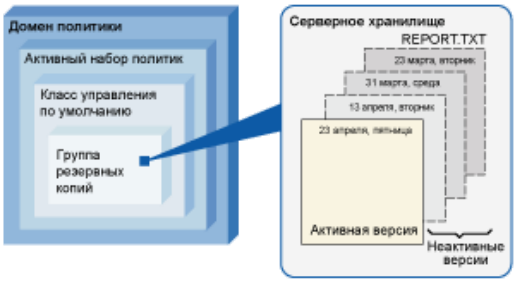


Табл. 2. Влияние политики на хранение версий резервных копий REPORT.TXT на 24 апреля

Резервные копии	Удаленные резервные копии	Оставить лишние резервные копии	Оставить удаленные резервные копии	Результаты
4 версии	2 версии	60 дней	180 дней	Параметры Резервные копии и Оставить лишние резервные копии управляют окончанием срока действия версий. Версия, созданная 23 марта, хранится до следующего резервного копирования этого файла (при этом создается четвертая неактивная версия) или пока не окажется, что эта версия оставалась неактивной в течение 60 дней. Если пользователь удалит файл REPORT.TXT с клиентской файловой системы, то сервер обнаружит удаление при выполнении следующей операции полного инкрементного резервного копирования клиента. С этого момента параметры Удаленные резервные копии и Оставить удаленные резервные копии также влияют на хранение. Теперь все версии неактивны. Две из четырех версий немедленно устареют (версии от 23 марта и 31 марта). Версия от 13 апреля устареет, когда она пробудет неактивной в течение 60 дней (23 июня). Сервер будет хранить последнюю неактивную версию от 23 апреля в течение 180 дней после того, как она станет неактивной.
Не ограничено	2 версии	60 дней	180 дней	Параметр Оставить лишние резервные копии управляет устареванием версий. Неактивные версии (кроме последней) устаревают после того, как пробудут неактивными в течение 60 дней. Если пользователь удалит файл REPORT.TXT с клиентского узла, сервер обнаружит удаление при выполнении следующей операции полного инкрементного резервного копирования клиента. С этого момента параметры Удаленные резервные копии и Оставить удаленные резервные копии также влияют на хранение. Теперь все версии неактивны. Две из четырех версий немедленно устареют (версии от 23 марта и от 31 марта), так как допускается только две версии. Версия от 13 апреля устареет, когда она пробудет неактивной в течение 60 дней (22 июня). Сервер будет хранить последнюю неактивную версию от 23 апреля в течение 180 дней после того, как она станет неактивной.

Резервные копии	Удаленные резервные копии	Оставить лишние резервные копии	Оставить удаленные резервные копии	Результаты
Не ограничено	Не ограничено	60 дней	180 дней	Параметр Оставить лишние резервные копии управляет устареванием версий. Сервер не вызывает устаревание неактивных версий на основании максимального количества резервных копий. Неактивные версии (кроме последней) устаревают после того, как пробудут неактивными в течение 60 дней. Если пользователь удалит файл REPORT.TXT с клиентского узла, сервер обнаружит удаление при выполнении следующей операции полного инкрементного резервного копирования клиентского узла. С этого момента параметр Оставить удаленные резервные копии также будет влиять на хранение. Теперь все версии неактивны. Три из четырех версий устареют после того, как каждая из них пробудет неактивной в течение 60 дней. Сервер будет хранить последнюю неактивную версию от 23 апреля в течение 180 дней после того, как она станет неактивной.
4 версии	2 версии	Не ограничено	Не ограничено	Параметр Резервные копии будет управлять устареванием версий до тех пор, пока пользователь не удалит файл с клиентского узла. Сервер не вызывает устаревание неактивных версий на основании срока хранения файла. Если пользователь удалит файл REPORT.TXT с клиентского узла, сервер обнаружит удаление при выполнении следующей операции полного инкрементного резервного копирования клиентского узла. С этого момента устареванием управляет параметр Удаленные резервные копии. Теперь все версии неактивны. Две из четырех версий немедленно устареют (версии от 23 марта и от 31 марта), так как допускается только две версии. Сервер хранит две оставшиеся неактивные версии неопределенный срок.

Информация, связанная с данной:

Полное и частичное инкрементное резервное копирование

Взаимодействия между параметрами политики

Параметры политики на основе времени и на основе версий взаимодействуют при совместном использовании в классе управления для политики. Частота резервного копирования клиента также влияет на версии резервных копий, которые хранятся для клиента.

В случае системы клиента, для которой резервное копирование должно производиться дважды в день, рассмотрите влияние следующих параметров политики на файл, который часто изменяется:

- Вы задали для параметра Оставить лишние резервные копии значение, равное 30 дням. Вы задаете значение Не ограничено для параметра Резервные копии, чтобы эта политика не ограничивала число версий. По истечении 30 дней на сервере может быть 60 версий резервных копий файла, если файл изменяется в интервале между двумя ежедневными операциями резервного копирования. Клиент может выбрать восстановление любой из 60 версий за последние 30 дней.
- Вы задаете значение Не ограничено для параметра Оставить лишние резервные копии и задаете для параметра Резервные копии значение, равное 30 версиям. Если файл изменится в промежутке между двумя каждыми ежедневными операциями резервного копирования, у сервера через 15 дней будет 30 версий резервных копий. По

истечении 30 на сервере все равно будет только 30 версий резервных копий из-за предельного числа версий. Если файл продолжит изменяться в промежутке между двумя каждыми ежедневными операциями резервного копирования, версии резервных копий могут оказаться только за последние 15 дней. Клиент может выбрать восстановление одной из 30 версий, возраст каждой из которых не превышает 15 дней.

В примерах показано, что, если версии резервных копий должны быть доступны в течение заданного числа дней, самый простой способ реализовать это - потребовать использовать политику на основе времени. Задайте для параметра Оставить лишние резервные копии определенное число дней и задайте для параметра Резервные копии значение Не ограничено.

Влияние значения Не ограничено в параметрах политики зависит от того, как заданы другие элементы управления политикой:

Оставить лишние резервные копии

Если задать значение Не ограничено, неактивные версии резервных копий будут удаляться на основе параметров Резервные копии или Удаленные резервные копии.

Чтобы разрешить клиентским узлам восстанавливать файлы на определенный момент времени, задайте для параметра Резервные копии или Удаленные резервные копии значение Не ограничено. Задайте в качестве значения параметра Оставить лишние резервные копии число дней, в течение которых, как вы ожидаете, клиентам могут понадобиться версии файлов, доступные для возможного моментального восстановления. Например, чтобы дать клиентам возможность восстанавливать файлы 60-дневной давности, задайте для параметра Оставить лишние резервные копии значение 60.

Оставить удаленные резервные копии

Если вы зададите значение Не ограничено, последняя версия будет храниться неограниченно долго, пока пользователь или администратор не удалит файл из серверного хранилища.

Резервные копии

Если задать значение Не ограничено, может потребоваться дополнительное пространство хранения, но в некоторых ситуациях это значение может быть необходимым. Например, чтобы разрешить клиентским узлам восстанавливать файлы на определенный момент времени, задайте для параметра Резервные копии значение Не ограничено. Если не задавать предельное число версий, сервер будет сохранять версии в соответствии с параметром Оставить лишние резервные копии.

Удаленные резервные копии

Если задать значение Не ограничено, может потребоваться дополнительное пространство хранения, но в некоторых ситуациях это значение может быть необходимым. Например, задайте для параметра Удаленные резервные копии значение Не ограничено, чтобы разрешить клиентам восстанавливать файлы на определенный момент времени. Если не задавать предельное число версий, сервер будет сохранять версии в соответствии с параметром Оставить лишние резервные копии.

Перекрестные ссылки для полей Центр операций и параметров командной строки сервера

В следующей таблице показаны поля Центр операций с эквивалентным параметром, который нужно использовать в команде `DEFINE COPYGROUP TYPE=BACKUP`.

Имя поля в представлениях Центр операций	**Параметр, который нужно использовать в команде `DEFINE COPYGROUP TYPE=BACKUP`**
Оставить лишние резервные копии	RETEXTRA
Оставить удаленные резервные копии	RETONLY
Резервные копии	VEREXISTS
Удаленные резервные копии	VERDELETED

Активация политики после обновления

При внесении обновлений в политику обновления не вступают в силу, пока вы не активируете обновленный набор политик.

При активации набора политик вступают в силу внесенные вами обновления. Например, после активации набора политик вступают в силу следующие типы обновлений:

- Вы задаете новый домен политики с набором политик и одним или несколькими классами управления
- Вы добавляете класс управления в набор политик
- Вы изменяете параметры хранения резервных копий в существующем классе управления

Проверка наборов политики перед активацией

В компоненте Центр операций проверка не является отдельным шагом. Если вы используете команды, проверка является дополнительной командой, которая дает возможность предварительно просмотреть результат активации измененного набора политик. При проверке набора политик сервер создает отчет об условиях, которые могли вызвать проблемы при активации набора политик.
Проверка завершится неудачно, если набор правил политики не содержит класса управления по умолчанию. При проверке появятся сообщения с предупреждениями, если выполняется любое из условий, показанных в Табл. 1.

Табл. 1. Условия, которые вызывают появление предупреждений при проверке набора политик

Условие	**Причина предупреждения**
Пункты назначения, указанные для операций резервного копирования, архивирования и переноса, не заданы для пулов хранения.	Чтобы пул хранения можно было задать как назначение, он должен существовать.
Пункт назначения хранилища, указанный для операций резервного копирования, архивирования или переноса, является пулом хранения копий или пулом активных данных.	Пунктом назначения хранилища должен быть первичный пул хранения.
Класс управления по умолчанию не содержит параметров резервных или архивных копий.	Если класс управления по умолчанию не содержит параметров резервных или архивных копий, ни резервное копирование, ни архивирование никаких файлов, связанных с классом управления по умолчанию, выполняться не будет.
Текущий активный набор политик указывает класс управления, который не задан в проверяемом наборе политик.	При создании резервных копий файлов, связанных с классом управления, которого больше не существует в активном наборе политик, резервные версии повторно связываются с классом управления по умолчанию. Если класса управления, с которым связана архивная копия, больше не существует, а класс управления по умолчанию не содержит параметров архивов, сервер будет управлять хранением архивной копии, используя льготный период хранения архивов. Льготный период хранения архивов задан для домена политики, и этот параметр используется, только если нет никаких других параметров политики для управления архивной копией.
Текущий активный набор политик содержит параметры резервных копий, не заданные в проверяемом наборе политик.	Если клиент создает резервную копию файла и у класса управления, с которым связан файл, больше нет параметров резервного копирования, версиями резервных копий будет управлять класс управления по умолчанию. Если класс управления по умолчанию не содержит никаких параметров резервных копий, сервер для управления версиями файлов будет использовать льготный период хранения резервных копий. Однако при выполнении следующей операции резервного копирования резервная копия файла создаваться не будет. Льготный период хранения резервных копий задан для домена политики, и этот параметр используется, только если нет никаких других параметров политики для управления версией резервной копии.

Условие	Причина предупреждения
Класс управления задает, что условием переноса файла с клиентского узла является наличие резервной версии, но этот класс не содержит параметров резервных копий.	Это предупреждение действует, только если вы используете продукт IBM Spectrum Protect for Space Management. Конфликты внутри класса управления могут привести к проблемам клиентов IBM Spectrum Protect for Space Management.

Активация набора политик

При активации набора политик сервер проверяет содержимое набора политик и копирует набор политик, так чтобы он стал активным набором политик. Потом, чтобы изменить содержимое активного набора политик, необходимо создать или изменить другой набор политик и активировать его.

Некоторые обновления политики сказываются немедленно при активации, но некоторые другие обновления - нет:

- Обновления параметров Оставить лишние резервные копии и Оставить удаленные резервные копии сразу же применяются к данным, которые уже есть в хранилище сервера, а также к последующим резервным копиям.

  Если вы используете команды, этими значениями являются параметры RETEXTRA и RETONLY для команды DEFINE COPYGROUP или UPDATE COPYGROUP.

- Обновления параметров Резервные копии и Удаленные резервные копии не вступают в силу для клиентских данных, пока клиенты не завершают следующую операцию резервного копирования.

  Если вы используете команды, этими значениями являются параметры VEREXISTS и VERDELETED для команды DEFINE COPYGROUP или UPDATE COPYGROUP.

Ограничения для серверов, использующих функцию защиты хранения данных

Если функция защиты хранения данных активна, при проверке и активации набора политик будет действовать больше правил. Функция защиты хранения данных активируется с помощью команды SET ARCHIVERETENTIONPROTECTION на сервере, на котором еще нет никаких данных клиента.

Если для сервера активна защита хранения данных, перед активацией политики должно быть выполнено больше правил:

- Если в активном наборе политик существует класс управления, то в активируемом наборе политик должен существовать класс управления с таким же именем.
- Все классы управления в наборе политик, который активируется, должны содержать параметры хранения архивов.
- Если у активного набора политик в классе управления есть параметры хранения архивов, у набора политик, который активируется, должны быть, как минимум, такие же значения хранения архивов, как соответствующие значения в активном наборе политик.

Если сервер является управляемым сервером в конфигурации предприятия, сервер должен получать обновления политики с сервера, который является менеджером конфигурации. Обновления политики, полученные управляемым сервером от менеджера конфигурации, также должны удовлетворять приведенным выше правилам.
Понятия, связанные с данным:
Конфигурирование на уровне предприятия (V7.1.1)
Ссылки, связанные с данной:
SET ARCHIVERETENTIONPROTECTION (включение защиты хранения данных)

Настройка политики

Вы можете настроить существующие политики, так чтобы они соответствовали новым или измененным требованиям к хранению данных в вашей организации. Изменение домена политики или копирование существующего домена политики - это стандартный способ начать настройку политики.

Об этой задаче

Ключевые параметры политики находятся в классах управления. В классах управления можно управлять как числом версий резервных копий, так и числом дней, в течение которого версии резервных копий хранятся в серверном хранилище. Если вы используете оба типа управления, политика будет более сложной. Управляя только сроком (в днях), в

течение которого хранятся версии резервных копий, вам будет проще задать, сколько времени хранятся резервные копии данных.

Убедитесь, что у класса управления по умолчанию в домене политики есть соответствующие параметры для хранения данных для большинства или для всех клиентов, назначенных в этот домен. Параметры хранения в классе управления применяются к данным, если для операций клиента не задан класс управления.

Вы можете работать над обновлениями политики и сохранить изменения на будущее. Когда вы решите, что черновые изменения готовы, вы можете активировать обновленный набор политик, чтобы изменения вступили в силу.

Процедура

1. На странице Обзор в компоненте Центр операций щелкните по меню Службы.
2. Выберите домен политик и щелкните по Подробности. Щелкните по Наборы политики.
3. Щелкните по переключателю Конфигурировать , чтобы можно было обновить параметры.
4. Настройте параметры в классе управления.
    a. Выберите параметры для служб резервного копирования. Например, обновите следующие элементы, чтобы неактивные версии резервных копий для клиентов хранились в течение 30 дней:
        - Резервные копии: Нет ограничения
        - Оставить лишние резервные копии: 30 дней
        - Удаленные резервные копии: 1
        - Оставить удаленные резервные копии: Нет ограничений
    b. Необязательно: Выберите параметры для служб архивирования. Например, измените значение параметра Хранить архивы на 1 год.
    c. Щелкните по Сохранить.
5. Необязательно: Щелкните по +Класс управления, чтобы добавить класс управления.
    a. Выберите базовые параметры и нажмите на Добавить.
    b. Настройте дополнительные параметры в новом классе управления. Для служб резервного копирования сделайте выбор в следующих столбцах: Назначение резервных копий, Резервные копии, Хранить дополнительные резервные копии, Удаленные резервные копии и Хранить удаленные резервные копии. Для служб архивирования сделайте выбор в столбцах Назначение архива и Хранить архивы.
    c. Щелкните по Сохранить.
6. Убедитесь, что в столбце По умолчанию в качестве класса управления по умолчанию выбран соответствующий класс управления. Параметры хранения в классе управления применяются, если для операций клиента не задан класс управления. Класс управления можно указать при выполнении операции клиента. Класс управления также можно задать в файле опций клиента, который находится в системе клиента, или в наборе опций клиента, заданном на сервере.
7. Активируйте набор политик, для чего щелкните по Активировать.
8. Назначьте клиентские узлы новому домену политики, либо обновив существующие клиентские узлы, либо зарегистрировав новые узлы.
    - Чтобы добавить новые клиенты в домен политики, щелкните по +Клиент.
    - Чтобы переместить существующий клиент в домен политики, выберите клиент, щелкните по Сведения и щелкните по вкладке Свойства. Выберите новый домен политики и щелкните по Сохранить.

    Хранение данных для клиента, назначенного вами в домен политики, теперь управляется этой политикой.
    Требование: Если клиент работает, когда вы назначаете для него новый домен, то, чтобы изменение вступило в силу, нужно остановить и перезапустить клиент.

Задачи, связанные с данной:
Управление операциями клиента через наборы опций клиентов

Создание политики путем копирования существующей политики

Вы можете создавать политики, копируя существующие политики, а затем изменяя части, которые вы хотите изменить.

Процедура

Вы можете создать политику, скопировав домен политики, обновив классы управления и назначив клиенты для нового домена.

1. На странице Обзор компонента Центр операций поместите указатель мыши на значок параметров  и выберите Построитель команд.

2. Скопируйте домен политики при помощи команды COPY DOMAIN. Например, скопируйте домен политики по умолчанию, STANDARD, в новый домен NEWDOMAIN:

   ```
   copy domain standard newdomain
   ```

   Эта операция позволяет скопировать домен политики и все связанные наборы политик и классы управления. В этом примере операция копирует следующие элементы в домен политики NEWDOMAIN:
   - Набор политик STANDARD.
   - Класс управления с именем STANDARD, который находится в наборе политик STANDARD.
   - Группы копий, содержащиеся в классе управления STANDARD:
     - Группа резервных копий STANDARD
     - Группа архивных копий STANDARD
3. На странице Обзор в компоненте Центр операций щелкните по меню Службы.
4. Выберите новый домен политики и щелкните по Подробности. Щелкните по Наборы политики.
5. Щелкните по переключателю Конфигурировать , чтобы можно было обновить параметры.
6. Настройте параметры в классах управления.
   a. Выберите параметры для служб резервного копирования. Например, обновите следующие элементы, чтобы неактивные версии резервных копий для клиентов хранились в течение 30 дней:
      - Резервные копии: Нет ограничения
      - Оставить лишние резервные копии: 30 дней
      - Удаленные резервные копии: 1
      - Оставить удаленные резервные копии: Нет ограничений

   b. Необязательно: Выберите параметры для служб архивирования. Например, измените значение параметра Хранить архивы на 1 год.
   c. Щелкните по Сохранить.
7. Необязательно: Внесите другие обновления и дополнения, например, добавьте класс управления.
   a. Щелкните по +Класс управления, чтобы добавить класс управления. Выберите базовые параметры и нажмите на Добавить.
   b. Настройте дополнительные параметры в новом классе управления. Для служб резервного копирования сделайте выбор в следующих столбцах: Назначение резервных копий, Резервные копии, Хранить дополнительные резервные копии, Удаленные резервные копии и Хранить удаленные резервные копии. Для служб архивирования сделайте выбор в столбцах Назначение архива и Хранить архивы.
   c. Щелкните по Сохранить.
8. Выберите класс управления по умолчанию, используемый клиентами, что будет указано в столбце По умолчанию. Щелкните по Сохранить. Параметры хранения в классе управления применяются, если для операций клиента не задан класс управления. Класс управления можно указать при выполнении операции клиента. Класс управления также можно задать в файле опций клиента, который находится в системе клиента, или в наборе опций клиента, заданном на сервере.
9. Активируйте набор политик, для чего щелкните по Активировать.
10. Назначьте клиентские узлы новому домену политики, либо обновив существующие клиентские узлы, либо зарегистрировав новые узлы.
    - Чтобы добавить новые клиенты в домен политики, щелкните по +Клиент.
    - Чтобы переместить существующий клиент в домен политики, выберите клиент, щелкните по Сведения и щелкните по вкладке Свойства. Выберите новый домен политики и щелкните по Сохранить.

    Хранение данных для клиента, назначенного вами в домен политики, теперь управляется этой политикой. Например, если вы реализовали пример в шаге 6, неактивные версии резервных копий для клиентов будут, по умолчанию, храниться 30 дней.
    Требование: Если клиент работает, когда вы назначаете для него новый домен, то, чтобы изменение вступило в силу, нужно остановить и перезапустить клиент.

Задачи, связанные с данной:
Управление операциями клиента через наборы опций клиентов

Создание домена политики

Вам может потребоваться создать новый домен политики для каждого типа клиента, защищенного сервером. Вам также может понадобиться разделить обязанности для клиентов среди нескольких администраторов, предоставив им полномочия на доступ к определенным доменам политики.

Об этой задаче

Создание нового домена политики может оказаться полезным в следующих обстоятельствах:

- Для приложений, систем или виртуальных машин требуются разные параметры хранения данных. Можно создать домен политики для каждого типа клиентов, используя политику по умолчанию, подходящую для этого типа.
- Администраторы отвечают за разные группы клиентов. Для каждого администратора можно создать домен политики, в который вы назначите клиентов, которые будут управляться этим администратором.

Процедура

В приведенных ниже шагах просуммировано, как создать домен политики.

1. На странице Обзор в компоненте Центр операций установите указатель мыши на значок параметров  и щелкните по Построитель команд.
2. Задайте домен политики при помощи команды DEFINE DOMAIN.
3. Задайте набор политик для домена, используя команду DEFINE POLICYSET.
4. На странице Обзор в компоненте Центр операций щелкните по меню Службы.
5. Выберите домен политик и щелкните по Подробности. Щелкните по Наборы политики.
6. Щелкните по переключателю Конфигурировать , чтобы можно было обновить параметры.
7. Щелкните по +Класс управления, чтобы добавить класс управления. Выберите базовые параметры и нажмите на Добавить.
8. Необязательно: Настройте дополнительные параметры в новом классе управления:
    a. Для служб резервного копирования сделайте выбор в следующих столбцах: Назначение резервных копий, Резервные копии, Хранить дополнительные резервные копии, Удаленные резервные копии и Хранить удаленные резервные копии.
    b. Для служб архивирования сделайте выбор в столбцах Назначение архива и Хранить архивы.
    c. Щелкните по Сохранить.
9. Необязательно: Щелкните по +Класс управления, чтобы добавить еще классы управления.
10. Убедитесь, что в столбце По умолчанию выбран класс управления по умолчанию.
11. Активируйте набор политик, для чего щелкните по Активировать.
12. Назначьте клиенты в новый домен политики. В строке меню Центр операций щелкните по Клиенты.
    - Чтобы добавить новые клиенты в домен политики, щелкните по +Клиент.
    - Чтобы переместить существующий клиент в домен политики, выберите клиент, щелкните по Сведения и щелкните по вкладке Свойства. Выберите новый домен политики и щелкните по Сохранить.

Ссылки, связанные с данной:
DEFINE DOMAIN (назначение нового домена политик)
DEFINE POLICYSET (Задать набор правил политики)

Управление операциями клиента через наборы опций клиентов

Наборы опций клиентов можно использовать, чтобы централизованно управлять опциями обработки, используемых клиентами для таких операций, как резервное копирование. Наборы опций клиентов помогают убедиться, что данные непротиворечивым образом защищены в соответствии с вашими требованиями. Набор опций клиента может переопределить опции в локальном файле опций клиента и может добавить опции, которых нет в локальном файле опций клиента.

Об этой задаче

Создавая и назначая наборы опций клиентов, вы сокращаете необходимость обновлять файлы локальных опций клиента и уменьшаете объем работы для вас или ваших пользователей.

Например, можно задать набор опций клиента, чтобы указать список включения-исключения, определяющий то, что включается в резервное копирование, а что из него исключается, а также какие классы управления используются для управления хранением данных. Другие опции клиента, которые могут быть полезны для централизованного управления в наборе опций клиента - это опции compression и deduplication.

Вы можете создавать наборы опций клиента для клиентов с аналогичными требованиями, например, для клиентов в одной и той же операционной системе, клиентов, использующих одну и ту же программу, или клиентов, используемых одним отделом. Например, вы можете создать наборы опций клиента для рабочих станций Windows или для отдела по выплате зарплаты. После создания набора опций клиентов вы назначаете набор опций клиента каждому всем клиентам одного и того же типа.

В наборе опций клиента на сервере можно задать не все опции клиента. Чтобы узнать об опциях клиента, которыми можно централизованно управлять в наборе опций клиента, смотрите раздел Опции клиента, которые может задавать

сервер.

Процедура

1. Задайте набор опций клиента при помощи команды DEFINE CLOPTSET. Например, чтобы задать набор опций клиента PAYROLLBACKUP, введите следующую команду:

   ```
   define cloptset payrollbackup description='Опции резервного копирования для отдела по выплате зарплаты'
   ```

2. Добавьте опции клиента в набор опций клиента с помощью команды DEFINE CLIENTOPT. Например, вы хотите добавить опции include и exclude в набор опций клиента PAYROLLBACKUP, чтобы добиться следующих целей:
   - Исключить из операций резервного копирования файлы временных Интернет-каталогов
   - Включить в операции резервного копирования все файлы в каталоге C:\Data и его подкаталогах и назначить для файлов класс управления PAYCLASS для хранения данных

   Введите следующие команды:

   ```
   define clientopt payrollbackup inclexcl "exclude.dir '*:\...\Временные Интернет-файлы'"
   define clientopt payrollbackup inclexcl "include C:\Data\...\* payclass"
   ```

3. Чтобы назначить набор опций клиента для клиента, выполните следующие шаги:
   a. На странице Обзор в компоненте Центр операций щелкните по Клиенты.
   b. Выберите клиент и щелкните по Подробности.
   c. Выберите Свойства.
   d. В области Общие выберите набор опций и щелкните по Сохранить.

Ссылки, связанные с данной:
DEFINE CLOPTSET (Определить имя набора опций клиента)
DEFINE CLIENTOPT (задать опцию для набора опций)
Информация, связанная с данной:
Опция клиента сжатия
Опция клиента дедупликации

Конфигурирование хранения

Выберите подходящий тип носителей в зависимости от того, какие функции хранения вам требуются. Оптимизируйте пулы хранения и управляйте ими для разных типов данных.

- Типы пулов хранения
  Чтобы помочь вам определить, какой тип пулов хранения лучше всего соответствует вашим требованиям к хранению, нужно оценить характеристики каждого типа пула хранения.
- Опции дедупликации данных
  Используйте встроенную дедупликацию данных, чтобы дедуплицировать данные и одновременно записывать их в пул хранения контейнера. Чтобы устранить дубликаты данных из пулов хранения с последовательным доступом (FILE), используйте дедупликацию данных после обработки.
- Конфигурирование устройств хранения
  Сконфигурируйте устройства хранения, подключив устройства, сконфигурировав драйверы устройств и создав на сервере объекты, соответствующие устройствам.
- Конфигурирование пула хранения каталога-контейнера для хранения данных
  Вы можете сконфигурировать пулы хранения каталогов-контейнеров, чтобы использовать встроенную дедупликацию данных для сохранения дедуплицированных данных.
- Конфигурирование пула хранения облачного контейнера для хранения данных
  Вы можете сохранять дедуплицированные и недедуплицированные данные в пуле хранения облачного контейнера и восстанавливать данные по мере необходимости.
- Управление пространством в пулах хранения контейнеров
  После того как вы сконфигурируете IBM Spectrum Protect и добавите пространство хранения, вы должны эффективно управлять своими данными и пространством пула хранения, чтобы они правильно функционировали. Используйте пулы хранения контейнеров, чтобы обеспечить максимальное пространство хранения и производительность сервера.
- Аудит пула хранения
  Можно запланировать операции аудита, чтобы идентифицировать запорченные файлы в пулах хранения.
- Аудит контейнера пула хранения
  Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе

данных и в контейнере в пуле хранения.

- Требования к системе хранения и уменьшение риска повреждения данных
  В случае сервера IBM Spectrum Protect можно использовать много типов хранения. Если вы используете дисковое хранилище блоков, твердотельные накопители (solid-state drive, SSD) или подключенные к сети файловые системы в качестве серверного хранилища, то убедитесь, что хранилище соответствует требованиям.

Типы пулов хранения

Чтобы помочь вам определить, какой тип пулов хранения лучше всего соответствует вашим требованиям к хранению, нужно оценить характеристики каждого типа пула хранения.

Чтобы оценить каждый тип пулов хранения, используйте следующую таблицу.

Тип пула хранения	**Описание**	**Использует**
Пул хранения каталога-контейнера	Первичный пул хранения, используемый сервером для хранения данных. Данные, хранящиеся в пулах хранения каталогов-контейнеров, используют либо встроенную дедупликацию данных, либо дедупликацию данных на стороне клиента. Облачный слой можно использовать для перемещения данных из пулов хранения каталогов-контейнеров в пулы хранения облачных контейнеров.	Используйте, если вы хотите произвести дедупликацию данных во встроенном режиме. Используя пулы хранения каталогов-контейнеров, вы избавляетесь от необходимости исправления томов, за счет чего повышается производительность сервера и снижается стоимость оборудования хранения. Использовать этот тип пулов хранения для операций резервного копирования, перенастройки, высвобождения, импорта или экспорта нельзя.
Пул хранения облачного контейнера	Первичный пул хранения, используемый сервером для хранения данных. Используйте пул хранения облачных контейнеров, чтобы хранить данные у провайдера облачного хранения на основе склада объектов. Данные, хранящиеся в пулах хранения облачных контейнеров, используют либо встроенную дедупликацию данных, либо дедупликацию данных на стороне клиента.	Сохраняя данные в пулах хранения облачных контейнеров, можно использовать преимущества более низкой стоимости за единицу, которые предлагает облако, вместе с возможностями масштабирования, обеспечиваемыми хранением в облаке. Использовать этот тип пулов хранения для операций резервного копирования, перенастройки, высвобождения, импорта или экспорта нельзя.
Пул хранения с произвольным доступом	Набор томов, которые сервер использует для хранения версий резервных копий файлов, файлов, представляющих собой архивные копии, и перенесенных файлов. Файлы хранятся на устройствах типа DISK.	Используйте этот тип пулов хранения, чтобы оставить копию данных на устройствах DISK. В пулы хранения следующих типов с произвольным или с последовательным доступом или из них можно переносить данные: • Пулы хранения с произвольным доступом • Пулы хранения с последовательным доступом

Тип пула хранения	Описание	Использует
Пул хранения с последовательным доступом	Набор томов, которые сервер использует для хранения версий резервных копий файлов, файлов, представляющих собой архивные копии, и файлов, перенесенных с клиентских узлов. Файлы хранятся на ленте или на устройствах типа FILE. Данные, хранящиеся в пулах хранения с последовательным доступом, используют как дедупликацию данных после обработки, так и дедупликацию данных на стороне клиента. Ограничение: Постобработка дедупликации данных доступна только в версии 7.1.2 и более ранних версиях.	Используйте этот тип пулов хранения, чтобы оставить копию данных на устройствах FILE и TAPE. В такой тип пулов хранения можно переносить данные.
Пул хранения копий	Именованный набор томов, содержащих копии файлов из первичного пула хранения. Пулы хранения копий используются только для резервного копирования данных, находящихся в первичных пулах хранения. Пул хранения копий не может быть пунктом назначения для группы резервных копий или архивных копий, а также для класса управления (для перенесенных файлов).	Используйте пулы хранения копий, чтобы у вас была копия активных и неактивных данных, которую можно восстановить в первичном пуле хранения после аварии или отключения питания. Использовать встроенную дедупликацию данных, сжатие, репликацию или дедупликацию данных в сочетании с этим типом пула хранения нельзя.
Пул хранения контейнера-копии	Набор ленточных томов, содержащих копии дедуплицированных экстентов, которые находятся в пулах хранения каталогов-контейнеров. Пулы хранения копий используются только для защиты данных, находящихся в пулах хранения каталогов-контейнеров. Пулы хранения контейнеров-копий используются для исправления повреждений в пуле хранения каталогов-контейнеров или для восстановления пулов хранения каталогов-контейнеров в случае аварии. Пулы хранения контейнеров-копий хранятся на носителях с последовательным доступом.	С помощью пулов хранения контейнеров-копий можно хранить копии пулов хранения каталогов-контейнеров локально или автономно. Поврежденные данные в пулах хранения каталогов-контейнеров можно восстановить при помощи дедуплицированных экстентов в пулах хранения контейнеров-копий.
Пул хранения активных данных	Именованный набор томов хранения, содержащий только активные резервные версии клиентских данных.	Используйте пулы хранения активных данных для восстановления только активных данных в первичные пулы хранения после аварии или отключения питания. Восстанавливая только активные данные, вы сможете быстрее восстановить данные клиента и будете использовать меньшую ширину полосы пропускания. Использовать встроенную дедупликацию данных, сжатие, репликацию или дедупликацию данных в сочетании с этим типом пула хранения нельзя.

Используйте следующую таблицу, чтобы сравнить возможности пулов хранения и выбрать пул хранения, который лучше всего соответствует вашим бизнес-требованиям, касающимся хранения.

Цель пользователя	Пул хранения каталога-контейнера	Пул хранения облачного контейнера	Пул хранения с произвольным доступом	Пул хранения с последовательным доступом	Пул хранения копий	Пул хранения контейнера-копии	Пул хранения активных данных
Защитить данные пулов хранения за счет репликации узлов.	✓		✓	✓	✓		✓
Сократить требования к хранению за счет использования встроенного сжатия.	✓	✓					
Сократить требования к хранению за счет использования встроенной дедупликации данных.	✓	✓					
Сократить требования к хранению за счет использования дедупликации данных на стороне клиента.	✓	✓		✓			
Сократить требования к хранению за счет использования дедупликации данных после обработки.				✓			
Защитить данные пулов хранения за счет защиты пулов хранения.	✓					✓	

Цель пользователя	Пул хранения каталога-контейнера	Пул хранения облачного контейнера	Пул хранения с произвольным доступом	Пул хранения с последовательным доступом	Пул хранения копий	Пул хранения контейнера-копии	Пул хранения активных данных
Создать резервные копии данных пула хранения данных, используя пулы хранения копий на диске или на ленте.			✓	✓			
Сохранить данные в облаке.		✓					
Используйте облачный слой для перемещения данных от пула хранения каталога-контейнера в пул хранения облачного контейнера.	✓						

Опции дедупликации данных

Используйте встроенную дедупликацию данных, чтобы дедуплицировать данные и одновременно записывать их в пул хранения контейнера. Чтобы устранить дубликаты данных из пулов хранения с последовательным доступом (FILE), используйте дедупликацию данных после обработки.

Для встроенной дедупликации данных следует использовать пулы хранения каталогов-контейнеров или пулы хранения облачных контейнеров. Используя пулы хранения каталогов-контейнеров или облачных контейнеров, вы избавляетесь от необходимости в автономной реорганизации, что позволяет повысить производительность сервера и снизить стоимость оборудования хранения. Для этих типов пулов хранения ни классы устройств, ни тома не используются.

При использовании дедупликации данных после обработки сервер сначала идентифицирует данные, а затем удаляет дубликаты данных в пул хранения. На носителе сохраняется только один экземпляр данных. Другие экземпляры тех же данных заменяются указателем на сохраненный экземпляр. При удалении дубликатов данных вы можете восстановить пространство в пуле хранения.

Дополнительную информацию о дедупликации данных после обработки смотрите в разделе Дедупликация данных (V7.1.1).

При дедупликации данных на стороне клиента на сервер отправляются только сжатые и дедуплицированные данные. Обработка распределяется между сервером и клиентом в процессе резервного копирования.

Чтобы сравнить опции дедупликации данных, используйте следующую таблицу.

Тип дедупликации данных	Преимущества	Недостатки

Тип дедупликации данных	Преимущества	Недостатки
Пост-обработка Ограничение: Используйте дедупликацию данных после обработки только для пулов хранения с последовательным доступом (FILE).	• После дедупликации данных можно высвободить пространство в пуле хранения.	• Более длительное время обработки, так как прежде чем удалять дедуплицированные данные из пула хранения, нужно идентифицировать данные.
Встроенная Ограничение: Встроенную дедупликацию данных можно использовать только для пулов хранения каталогов-контейнеров и облачных контейнеров.	• Дедуплицирует данные при их записи в пул хранения контейнеров. • Уменьшает необходимость в автономной реорганизации, что повышает производительность сервера. • Сокращает стоимость оборудования для хранения.	• Более высокая степень использования процессора сервером.
Сторона клиента	• Обработка распределяется между сервером и клиентом в процессе резервного копирования.	• Высокая степень использования процессора клиентом. • Длительное время выполнения клиентских операций, например резервного копирования. • На сервер отправляются только сжатые дедуплицированные данные.

- Определение правила для генерирования статистики дедупликации данных
  Можно задать правило генерировать статистику дедупликации данных по регулярному расписанию для указанных узлов, групп узлов и файловых пространств. Можно генерировать статистику в одно и то же время каждый день или в заданных интервалах.

Задачи, связанные с данной:
Конфигурирование дедупликации данных (дисковое решение с несколькими площадками)
Конфигурирование дедупликации данных (дисковое решение с одной площадкой)
Сравнение пулов хранения

Конфигурирование устройств хранения

Сконфигурируйте устройства хранения, подключив устройства, сконфигурировав драйверы устройств и создав на сервере объекты, соответствующие устройствам.

Об этой задаче

Если вы настраиваете новый диск для одного сайта, диска с несколькими сайтами или ленточного решения, вы можете найти информацию о конфигурировании устройств хранения в решениях по защите данных IBM Spectrum Protect.

Если вы не настраиваете новое решение, сконфигурируйте устройства хранения и управляйте ими, следуя инструкциям в документации по V7.1.1:

- Операционные системы AIXОперационные системы LinuxКонфигурирование и управление устройствами хранения
- Операционные системы WindowsКонфигурирование и управление устройствами хранения

Конфигурирование пула хранения каталога-контейнера для хранения данных

Вы можете сконфигурировать пулы хранения каталогов-контейнеров, чтобы использовать встроенную дедупликацию данных для сохранения дедуплицированных данных.

Процедура

Чтобы сохранить данные в пуле хранения каталога-контейнера, выполните следующие шаги:

1. Создайте пул хранения каталога-контейнера, сделав следующее:
   a. В строке меню компонента Центр операций выберите Хранение > Пулы хранения.
   b. На странице Пулы хранения щелкните по + Пул хранения.
   c. Выполните шаги в мастере Добавить пул хранения. В качестве типа хранения на основе контейнеров выберите значение Каталог.
2. После того как мастер создаст пул хранения, обновите классы управления и наборы политик, чтобы использовать новый пул. Чтобы обновить класс управления для использования нового пула, выполните следующие действия:
   a. В панели меню компонента Центр операций выберите Службы.
   b. На странице Политики выберите домен политики и щелкните по Сведения.
   c. На странице Сведения щелкните по вкладке Наборы политики.
   d. Щелкните по переключателю Конфигурировать. Теперь наборы политик доступны для изменения.
   e. Необязательно: Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
   f. Обновите один или несколько классов управления, чтобы использовать новый пул, изменив поле Назначение резервного копирования в таблице.
   g. Щелкните по Сохранить.
3. Активируйте измеренный набор политик, выполнив следующие шаги:
   a. Выберите Активировать. Поскольку изменение активного набора политик может привести к потере данных, будет показана сводка различий между активным набором политик и новым набором политик.
   b. Проверьте разницу между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном в настоящий момент наборе политик, после активации будут связаны с классами управления с такими же именами в новом наборе политик.
   c. Укажите в активном в настоящий момент наборе политик классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут после активации управляться классом управления по умолчанию в новом наборе политик.
   d. Если изменения, реализуемые набором политики, являются допустимыми, выберите переключатель Я понимаю, что эти обновления могут вызвать потерю данных и щелкните по Активировать.
4. Щелкните по переключателю Конфигурировать. Теперь наборы политик больше нельзя изменять.

Дальнейшие действия

Чтобы защитить пул хранения каталогов-контейнеров, введите команду PROTECT STGPOOL. Инструкции смотрите в разделах PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения) и Копирование пулов хранения каталогов-контейнеров на ленту.

 Операционные системы LinuxЕсли вы защищаете пул хранения каталогов-контейнеров, копируя данные на удаленный сервер, и столкнулись с сетевыми ошибками, смотрите раздел Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде.

- Копирование пулов хранения каталогов-контейнеров на ленту
  Данные в пуле хранения каталога-контейнера можно защитить, скопировав данные в пулы хранения контейнеров-копий, представленных ленточными томами. Эта ленточная копия используется для исправления повреждений пула хранения каталогов-контейнеров.
- Перевод ленточных томов вне площадки, когда DRM не сконфигурирован
  Если в вашем решении по хранению есть пулы хранения контейнеров-копий, представленные ленточными томами, но вы не сконфигурировали функцию менеджера восстановления после аварий (DRM), вы можете вручную выполнить процедуру по переводу ленточных томов вне площадки. Обслуживая копии данных на ленточных томах вне площадки, вы сможете восстановить данные, если на площадке произойдет авария.
- Изменение порога высвобождения томов для пулов хранения контейнеров-копий
  По умолчанию высвобождение ленточных томов включено для пулов хранения контейнеров-копий. Чтобы обеспечить эффективное использование ленточных томов, измените порог высвобождения томов.
- Высвобождение ленточных томов в пулах хранения контейнеров-копий
  Вы можете высвободить ленточные тома в пулах хранения контейнеров-копий, не выполняя операцию защиты, если у вас нет времени на выполнение и операции по защите, и операции по высвобождению пространства.
- Как указать, следует ли использовать пулы хранения контейнеров-копий для защиты при авариях
  Определите, соответствуют ли пулы хранения контейнеров-копий требованиям к защите от аварий.

Копирование пулов хранения каталогов-контейнеров на ленту

Данные в пуле хранения каталога-контейнера можно защитить, скопировав данные в пулы хранения контейнеров-копий, представленных ленточными томами. Эта ленточная копия используется для исправления повреждений пула хранения каталогов-контейнеров.

Прежде чем начать

Задайте на сервере хотя бы одну ленточную библиотеку при помощи команды DEFINE LIBRARY. В ней должно быть достаточно ленточных устройств и чистых томов, чтобы соответствовать вашим потребностям хранения. Дополнительную информацию об управлении носителями резервных копий и конфигурировании менеджера аварийного восстановления (disaster recovery manager, DRM) смотрите в разделе Менеджер аварийного восстановления (V7.1.1).

Об этой задаче

Для копирования данных в пулах хранения каталогов-контейнеров на ленту Центр операций создает расписание запуска команды PROTECT STGPOOL. При запуске расписания защиты создается одна ленточная копия. При запуске расписания защиты должен быть доступен хотя бы один том. В противном случае операция перемещения выполнена не будет.

Можно создать до двух ленточных копий, но для создания второго пула хранения контейнера-копии следует использовать интерфейс командной строки. Одну ленточную копию можно перенести вне сайта, чтобы обеспечить возможность восстановления после аварии. Другую копию можно оставить локальной для облегчения восстановления после менее серьезных ошибок.

ограничения:

- Виртуальные библиотеки на лентах не поддерживаются вне зависимости от того, какой тип библиотеки определен. Поддерживаются только физические ленты.
- Пулы хранения контейнеров-копий могут использоваться для исправления небольших или средних повреждений пулов хранения, включая повреждения контейнеров и каталогов. Пулы хранения контейнеров-копий также можно использовать для защиты от аварий, но вы должны убедиться, что время восстановления соответствует вашим требованиям. Дополнительные сведения смотрите в разделе Как указать, следует ли использовать пулы хранения контейнеров-копий для защиты при авариях.
- Использовать репликацию для целевого пула хранения контейнера-копии нельзя.
  Совет: Вы можете создать ленточную копию данных пула хранения каталога-контейнера на сайте аварийного восстановления, используя эту процедуру для создания пула хранения контейнера-копии на целевом сервере репликации. Затем запланируйте выполнение команд PROTECT STGPOOL и REPLICATE NODE на исходном сервере репликации, чтобы защитить ваши данные на целевом сервере репликации.
- Описанную процедуру нельзя использовать, если с пулом хранения каталогов-контейнеров уже связан пул хранения контейнеров-копий. Чтобы создать второй пул хранения контейнеров-копий, выполните инструкции в разделе 5.

Если вы создали пул хранения контейнеров-копий как часть мастера Добавить пул хранения, в этой процедуре нет необходимости. После завершения работы мастера Центр операций сконфигурирует пул хранения контейнера-копии и расписание защиты.

Процедура

Чтобы сконфигурировать защиту пула хранения с копированием на ленту для существующего пула хранения каталогов-контейнеров, выполните следующие действия:

1. В строке меню компонента Центр операций выберите Хранение > Пулы хранения.
2. На странице Пулы хранения выберите пул хранения каталогов-контейнеров, для которого требуется защита с копированием на ленту.
3. Выберите Еще > Добавить пул контейнеров-копий.
4. Выполните инструкции в окне Добавить пул контейнеров-копий, чтобы запланировать защиту с копированием на ленту.
5. Выполнив предыдущие шаги, можно добавить второй пул хранения контейнеров-копий, используя интерфейс командной строки. Дополнительно, выполните следующие действия, чтобы добавить пул хранения контейнеров-копий:
   a. Создайте пул хранения контейнеров-копий при помощи команды DEFINE STGPOOL.

b. Назначьте этот пул хранения контейнеров-копий пулу хранения каталогов-контейнеров командой UPDATE STGPOOL для пула каталогов-контейнеров.

Результаты

После завершения конфигурирования данные в пуле хранения каталога-контейнера копируются в пул хранения контейнера-копии в соответствии с заданным расписанием защиты.

Дальнейшие действия

1. Если вы создали ленточную копию для хранения вне сайта, включите внесайтовый пул хранения контейнера-копии для операций DRM, введя команду SET DRMCOPYCONTAINERSTGPOOL. Убедитесь, что ленточные тома добавлены в расписания ротации лент вне сайта. Если DRM не сконфигурирован, нужно это сделать или следует воспользоваться альтернативным методом перемещения лент в удаленное положение. Инструкции по альтернативному методу смотрите в разделе Перевод ленточных томов вне площадки, когда DRM не сконфигурирован. Чтобы убедиться, что дистанционные пулы хранения контейнеров-копий включены для DRM, воспользуйтесь командой QUERY DRMSTATUS.

   Инструкции по конфигурированию DRM смотрите в документе Disaster recovery manager (V7.1.1.

2. Убедитесь, что порог высвобождения для пула хранения контейнера-копии соответствует вашим требованиям.

   По умолчанию высвобождение ленточных томов включено для новых пулов хранения контейнеров-копий, созданных с использованием компонента Центр операций. Высвобождение тома происходит, когда порог высвобождения для пула хранения контейнеров-копий меньше 100%. Однако ленточные тома не являются кандидатами для высвобождения, пока они не заполнены на 75%. При использовании высвобождения для пулов хранения контейнеров-копий, у которых есть тома вне сайта, действуйте с осторожностью. Когда том вне сайта становится подлежащим высвобождению, сервер перемещает экстенты с тома обратно в расположение на сайте. Если авария происходит локально, то сервер сможет получить экстенты с удаленного тома, если у восстановленной базы данных есть ссылки на экстенты на удаленном томе. Чтобы запретить немедленную перезапись томов после удаления всех экстентов, используйте параметр REUSEDELAY, чтобы задать значение, превышающее 0. Центр операций задает порог высвобождения, равный 60%, для пулов хранения контейнеров-копий, находящихся на сайте.

   Инструкции по изменению порога высвобождения смотрите в разделе Изменение порога высвобождения томов для пулов хранения контейнеров-копий.

3. Защитите метаданные для пула хранения контейнера-копии.
   При выполнении расписания защиты экстенты данных в пулах хранения контейнеров-копий копируются на ленточные тома без связанных метаданных. Эти метаданные требуются для восстановления ленточных копий. Для защиты метаданных необходимо по отдельности выполнить резервное копирование базы данных сервера, а также файлов хронологии тома, опций сервера и файлов конфигурации устройств. Если используется консолидация для пулов хранения контейнеров-копий, содержащих удаленные ленточные тома, убедитесь, что для обеспечения защиты аварийного восстановления выполнены следующие требования:
   - Резервное копирование баз данных запускается после выполнения расписаний защиты пулов хранения и расписаний перемещения DRM.
   - Все тома резервных копий баз данных и тома DRM переносятся в удаленное положение вместе.

   Инструкции по резервному копированию базы данных сервера смотрите в разделе Как задать расписания для операций по обслуживанию сервера.

4. (Необязательно) Измените расписание защиты для пула хранения каталога-контейнера, у которого есть один или несколько связанных пулов хранения контейнеров-копий, используя команду UPDATE SCHEDULE. Имя расписания, созданного компонентом Центр операций - CONTAINER_COPY.

Понятия, связанные с данным:
Хранение данных в пулах хранения контейнеров-копий
Задачи, связанные с данной:
Как указать, следует ли использовать пулы хранения контейнеров для защиты при авариях
Ссылки, связанные с данной:
DEFINE LIBRARY (Задать библиотеку)
PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения)
UPDATE SCHEDULE (изменение административного расписания)
QUERY DRMSTATUS (Запросить системные параметры менеджера аварийного восстановления)

Перевод ленточных томов вне площадки, когда DRM не сконфигурирован

Если в вашем решении по хранению есть пулы хранения контейнеров-копий, представленные ленточными томами, но вы не сконфигурировали функцию менеджера восстановления после аварий (DRM), вы можете вручную выполнить процедуру по переводу ленточных томов вне площадки. Обслуживая копии данных на ленточных томах вне площадки, вы сможете восстановить данные, если на площадке произойдет авария.

Процедура

1. Зарезервируйте том хранения, который нужно перевести вне площадки, используя команду CHECKOUT LIBVOLUME.
2. Обновите том, чтобы указать, что он переводится вне площадки, введя команду UPDATE VOLUME и указав `ACCESS=OFFSITE`. (Необязательно) Укажите расположение вне площадки, используя параметр LOCATION. Например, укажите `LOCATION=SITE1`.
3. Высвободите (консолидируйте) пространство, выполнив одно из следующих действий:
   - Чтобы высвободить пространство, не защищая пул хранения, введите команду PROTECT STGPOOL и укажите `TYPE=LOCAL` и `RECLAIM=ONLY`.
   - Чтобы высвободить пространство, защищая пул хранения, введите команду PROTECT STGPOOL, не указывая параметр RECLAIM.
4. Отслеживайте том при помощи команды QUERY VOLUME. Если том показан как недоступный и пустой, верните том на площадку и активируйте его в библиотеке, используя команду CHECKIN LIBVOLUME.
5. Обновите том, введя команду UPDATE VOLUME и указав `ACCESS=READWRITE`.

Ссылки, связанные с данной:
CHECKOUT LIBVOLUME (исключение тома хранения из библиотеки)
PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения)
UPDATE VOLUME (изменение тома пула хранения)

Изменение порога высвобождения томов для пулов хранения контейнеров-копий

По умолчанию высвобождение ленточных томов включено для пулов хранения контейнеров-копий. Чтобы обеспечить эффективное использование ленточных томов, измените порог высвобождения томов.

Процедура

1. Щелкните на странице Обзор в компоненте Центр операций по Хранение > Пулы хранения.
2. Выберите пул хранения и нажмите кнопку Сведения, а затем щелкните по Свойства.
3. В разделе Высвобождение задайте процент высвобождения и нажмите кнопку Сохранить.
   Совет: Другой вариант - изменить процент высвобождения при помощи команды UPDATE STGPOOL, задав для нее параметр RECLAIM. Подробную информацию о параметре RECLAIM смотрите в описании команд, позволяющих задать и обновить пулы хранения контейнеров-копий.
   Ограничение: Команду RECLAIM STGPOOL нельзя использовать для высвобождения томов в пулах хранения контейнеров-копий. Подробную информацию о высвобождении томов в пулах хранения контейнеров-копий смотрите в описании параметра RECLAIM в команде PROTECT STGPOOL.

Высвобождение ленточных томов в пулах хранения контейнеров-копий

Вы можете высвободить ленточные тома в пулах хранения контейнеров-копий, не выполняя операцию защиты, если у вас нет времени на выполнение и операции по защите, и операции по высвобождению пространства.

Об этой задаче

При вводе команды PROTECT STGPOOL, если целевой пул хранения является пулом хранения контейнеров-копий, по умолчанию выполняется и операция защиты, и операция высвобождения. Предпочтительная практика - разрешить выполнение и операции защиты, и операции высвобождения. Однако, чтобы сэкономить время, можно выполнить только

операцию защиты пула хранения или только операцию высвобождения, либо можно ограничить число высвобождаемых ленточных томов. Используйте эту процедуру, только если вам нужно быстро высвободить ленточные тома или нужно высвободить ограниченное число ленточных томов.

Процедура

Чтобы высвободить ленточные тома, не выполняя операцию по защите пула хранения, сделайте следующее:

1. Необязательно: Чтобы довести до максимума объем высвобождаемого пространства, запустите процесс удаления устаревших объектов из перечня, введя команду EXPIRE INVENTORY.
2. Решите, хотите ли вы, чтобы высвобождение пространства выполнялось до завершения, или хотите ограничить число высвобождаемых ленточных томов.
3. Чтобы запустить высвобождение до его завершения, введите команду PROTECT STGPOOL и задайте параметры TYPE=LOCAL и RECLAIM=ONLY. Например, чтобы высвободить пространство в локальном пуле хранения контейнера-копии, заданном в качестве целевого пула защиты для SPOOL1, введите следующую команду:

   ```
   protect stgpool spool1 type=local reclaim=only
   ```

4. Чтобы высвободить ограниченное число ленточных томов, выполните следующие шаги:
   a. Задайте предел высвобождения для пула хранения контейнера-копии, введя команду UPDATE STGPOOL с параметром RECLAIMLIMIT. Этот параметр ограничивает число томов в пуле хранения контейнеров-копий, которые высвобождаются.
   b. Введите команду PROTECT STGPOOL и задайте параметр TYPE=LOCAL, указав вместе с ним либо параметр RECLAIM=YESLIMITED, либо параметр RECLAIM=ONLYLIMITED.
   Совет: Если вы зададите RECLAIM=YESLIMITED, и операция высвобождения, и операция защиты пула хранения будут выполнены при вводе команды PROTECT STGPOOL. Если вы зададите RECLAIM=ONLYLIMITED, высвобождение будет единственной выполняемой операцией. Если вы зададите любое из этих значений, высвобождение будет выполняться, только пока не будет достигнут предел высвобождения, заданный для пула хранения контейнера-копии. Предел высвобождения назначается с помощью параметра RECLAIMLIMIT в команде DEFINE STGPOOL или UPDATE STGPOOL.

   Например, чтобы высвободить предельное число ленточных томов, равное пяти, в пуле хранения контейнера-копии CCPOOL1, не выполняя операцию защиты для исходного пула хранения каталога-контейнера SPOOL1, введите следующие команды:

   ```
   update stgpool ccpool1 reclaimlimit=5
   protect stgpool spool1 type=local reclaim=onlylimited
   ```

   Например, чтобы защитить пул хранения SPOOL1 и высвободить ленточные тома, максимальное число которых может достигать 10, в связанном пуле хранения контейнера-копии, введите следующую команду:

   ```
   update stgpool spool1 reclaimlimit=10
   protect stgpool spool1 type=local reclaim=yeslimited
   ```

Результаты

Обработка высвобождения для этого пула хранения контейнеров-копий завершается. Операция защиты пула хранения не выполнялась, так что данные в пуле хранения каталога-контейнера, обновленного с момента последней операции защиты, не будут защищены.

Дальнейшие действия

1. Защитите данные в пуле хранения каталога-контейнера путем их переноса в пул хранения контейнера-копии, введя команду PROTECT STGPOOL и задав параметр TYPE=LOCAL. Процесс защиты выполняется с использованием параметра по умолчанию RECLAIM=YES. Операция защиты займет меньше времени, поскольку высвобождение уже выполнено.
   Например, чтобы защитить данные в пуле хранения каталога-контейнера с именем SPOOL1, введите следующую команду:

   ```
   protect stgpool spool1 type=local
   ```

   Либо, защитите данные в пуле хранения каталога-контейнера с именем SPOOL1, не выполняя высвобождение пространства; для этого введите следующую команду:

   ```
   protect stgpool spool1 type=local reclaim=no
   ```

2. Создайте резервную копию базы данных сервера и запустите запланированные операции обслуживания. Инструкции смотрите в разделе Как задать расписания для операций по обслуживанию сервера.

Ссылки, связанные с данной:
PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения)
DEFINE STGPOOL (Задать пул хранения контейнера-копии)
UPDATE STGPOOL (Задать пул хранения контейнера-копии)
EXPIRE INVENTORY (ручной запуск обработки устаревания перечня)

Как указать, следует ли использовать пулы хранения контейнеров-копий для защиты при авариях

Определите, соответствуют ли пулы хранения контейнеров-копий требованиям к защите от аварий.

Об этой задаче

Можно создать внесайтовую копию пула хранения контейнеров-копий, чтобы можно было произвести восстановление при авариях или чтобы выполнить нормативные требования и бизнес-требования к внесайтовым ленточным копиям. Прежде чем вы решите использовать внесайтовые ленточные копии для защиты при авариях, внимательно рассмотрите вопрос, соответствует ли решение вашим целям по экономии времени.

Использование пулов хранения контейнеров-копий для аварийного восстановления подходит, если объем данных в вашей среде меньше или равен следующим значениям:

- 200 ТБ общего объема управляемых данных
- 50 ТБ внутренних данных
- 37 ТБ фронтальных данных

Общий объем управляемых данных
: Все данные, которые хранятся в пуле хранения каталога-контейнера на сервере. Сюда входят как активные, так и неактивные версии данных. Число версий определяется политикой хранения.

Внутренние данные
: Все данные, которые хранятся в пуле хранения контейнера-копии.

Фронтальные данные
: Текущие активные данные, которые хранятся в пуле хранения контейнера-копии. Это активные данные, которые используются для восстановления данных на клиентских узлах. При аварии, чтобы восстановить производство, потребуются все фронтальные данные или их часть. Фронтальные данные - это процент общего объема управляемых данных, который меньше или равен общему объему управляемых данных в зависимости от используемых параметров политики.

Чтобы произвести восстановление после аварии в течение 48 часов, системная среда на сайте восстановления должна соответствовать минимальным требованиям к аппаратным средствам для выполнения действий в следующей таблице.

Действие	Необходимое время	Минимальные требования
Сконфигурируйте новый сервер IBM Spectrum Protect на сайте аварийного восстановления. Чтобы сконфигурировать новый сервер, нужно выполнить следующие шаги: 1. Предоставить диски для сервера. 2. Восстановить сервер из резервной копии. 3. Запустить сервер. 4. Обновить конфигурации хранения и устройств.	Время на восстановление сервера: 6 часов	Используйте для базы данных сервера твердотельный диск (solid-state drive, SSD), соответствующий следующим требованиям: • Средняя комбинированная пропускная способность чтения/записи не менее 100 МБ в секунду • Среднее число операций ввода-вывода в секунду (input/output operations per second, IOPS) не менее 12862.

Действие	Необходимое время	Минимальные требования
Произведите аудит пула хранения каталога-контейнера и восстановите данные с ленты. Совет: Если система соответствует минимальным требованиям к аппаратным средствам, вы сможете восстановить до 50 ТБ внутренних данных в течение 48 часов.	Время для аудита пула хранения: 2 часа Время для восстановления пула хранения с использованием ленточной копии: 28 часов Прим.: Оценка времени применяется, если у вас есть максимальный общий объем управляемых данных в пуле хранения, равный 200 ТБ.	Используйте накопители Nearline SAS (NL-SAS) как конфигурацию среднего проектируемого сервера с минимально производительностью записи на диск пула хранения, равной 700 МБ в секунду. Используйте ленточную технологию нового поколения, например, LTO-7 или новее, с минимальным числом накопителей, равным 6, чтобы разрешить параллельные операции чтения с ленточных томов.
Восстановите данные на клиентских узлах. Совет: Если система соответствует минимальным требованиям к аппаратным средствам, вы сможете восстановить до 37 ТБ фронтальных данных в течение 48 часов.	Время операций восстановления клиентов: 12 часов	Используйте накопители NL-SAS как конфигурацию среднего проектируемого сервера с минимальным числом сеансов восстановления, равным 10, достигая скорости 3102 ГБ в час.

Процедура

1. Оцените время восстановления после аварии для вашей среды, используя следующую таблицу. Определите, соответствует ли время восстановления вашим требованиям.

   Табл. 1. Оценка времени восстановления для разных общих объемов управляемых данных

Цель по времени восстановления	Общий объем управляемых данных (ТБ)	Время (в часах) исправления пула хранения каталога-контейнера (первый восстановленный байт)	Время в часах до восстановления клиентских узлов (аварийное восстановление завершено)
До 1 дня	25	10	12
	50	13	16
	75	17	22
До 2 дней	100	20	26
	200	34	46
До 4 дней	300	48	66
	400	62	86
Более 4 дней	500	76	106

   Примечания:
   - Достигаемые скорости сильно зависят от рабочей нагрузки и сконфигурированной среды.
   - Процент фронтальных данных относится к общему объему управляемых данных. При увеличении объема фронтальных данных увеличивается общее время восстановления. При уменьшении объема фронтальных данных общее время восстановления уменьшается.
2. Оцените время восстановления для вашей среды, используя следующие формулы:
   - Оцените значение **Время (в часах) исправления пула хранения каталога-контейнера (первый восстановленный байт)**:

     ```
     Время до восстановления первого байта клиента =
     6 часов + 14 часов для каждых 100 ТБ общих управляемых данных
     ```

   - Оцените значение **Время в часах до восстановления клиентских узлов (аварийное восстановление завершено)**:

     ```
     Время до полного восстановления клиента =
     Время до восстановления первого байта клиента + ((Общий объем управляемых данных *
     Фронтальные данные) / Скорость восстановления)
     ```

Скорость восстановления: Скорость, с которой клиенты могут восстановить данные с сервера обратно на свой локальный компьютер или устройство хранения.

3. Выполните тест-процедуры по аварийному восстановлению, чтобы можно было использовать пулы хранения контейнеров-копий для восстановления вашей среды в течение промежутка времени, соответствующего вашим требованиям.

Ссылки, связанные с данной:
Восстановление пулов хранения после аварии

Конфигурирование пула хранения облачного контейнера для хранения данных

Вы можете сохранять дедуплицированные и недедуплицированные данные в пуле хранения облачного контейнера и восстанавливать данные по мере необходимости.

Прежде чем начать

Ознакомьтесь с требованиями и ограничениями, касающимися пулов хранения облачных контейнеров.

Пулы хранения облачных контейнеров можно сконфигурировать для использования одного из следующих провайдеров услуг и протоколов:

- Amazon Web Services (AWS) с Simple Storage Service (S3)
- Microsoft Azure
- IBM® Cloud Object Storage с S3
- IBM Cloud Object Storage с S3 и IBM Cloud
- IBM Cloud Object Storage с Swift и IBM Cloud
- OpenStack с Swift с использованием Keystone версии 1 или 2

Ограничение: Пулы хранения облачных контейнеров не поддерживаются в операционной системе Linux on System z.
Получите информацию о конфигурации и задайте класс устройств, выполнив следующие шаги:

1. Получите информацию о конфигурации для вашего провайдера облачных услуг:
   - Amazon с S3 (не на месте)
   - Microsoft Azure
   - IBM Cloud Object Storage с S3 (не на месте, с IBM Cloud)
   - IBM Cloud Object Storage со Swift (не на месте, с IBM Cloud)
   - IBM Cloud Object Storage с S3 (на месте)
   - OpenStack со Swift (на месте или не на месте)
2. Задайте класс устройств для операций резервного копирования базы данных. При использовании шифрования для пулов хранения облачных контейнеров главный ключ шифрования сервера используется для защиты облачного ключа шифрования в резервной копии базы данных.
   a. В строке меню компонента Центр операций щелкните по Серверы.
   b. Выберите строку сервера и щелкните по Резервное копирование.
   c. Выберите класс устройств, который нужно использовать для операций резервного копирования базы данных, и щелкните по Резервное копирование.

   Совет: Либо используйте команду SET DBRECOVERY, чтобы задать класс устройства для резервного копирования базы данных.

Процедура

Чтобы сохранить данные в пуле хранения облачного контейнера, выполните следующие шаги:

1. Создайте пул хранения облачного контейнера. Вы должны задать информацию о конфигурации, идентифицирующую службу облака.
   a. В строке меню компонента Центр операций выберите Хранение > Пулы хранения.
   b. На странице Пулы хранения щелкните по + Пул хранения.
   c. Выполните шаги в мастере Добавить пул хранения. Выберите в качестве типа хранения на основе контейнеров значение Облако на месте или Облако вне системы.
2. Обновите классы управления и наборы политик, чтобы использовать новый пул хранения. Чтобы обновить класс управления для использования нового пула хранения, выполните следующие шаги:

a. В панели меню компонента Центр операций выберите Службы.
b. На странице Политики выберите домен политики и щелкните по Сведения.
c. На странице Сведения щелкните по вкладке Наборы политики.
d. Щелкните по переключателю Конфигурировать. Теперь наборы политик доступны для изменения.
e. Необязательно: Чтобы изменить неактивный набор политик, щелкните по стрелкам вперед и назад, чтобы найти набор политик.
f. Обновите один или несколько классов управления, чтобы использовать новый пул хранения, изменив поле Назначение резервного копирования в таблице.
g. Щелкните по Сохранить.

3. Активируйте измеренный набор политик, выполнив следующие шаги:
   a. Выберите Активировать. Поскольку изменение активного набора политик может привести к потере данных, будет показана сводка различий между активным набором политик и новым набором политик.
   b. Проверьте разницу между соответствующими классами управления в двух наборах политик и рассмотрите последствия для файлов клиентов. Файлы клиентов, связанные с классами управления в активном в настоящий момент наборе политик, после активации будут связаны с классами управления с такими же именами в новом наборе политик.
   c. Укажите в активном в настоящий момент наборе политик классы управления, у которых нет эквивалентов в новом наборе политики, и рассмотрите последствия для файлов клиента. Файлы клиентов, связанные с этими классами управления, будут после активации управляться классом управления по умолчанию в новом наборе политик.
   d. Если изменения, реализуемые набором политики, являются допустимыми, выберите переключатель Я понимаю, что эти обновления могут вызвать потерю данных и щелкните по Активировать.
4. Щелкните по переключателю Конфигурировать. Теперь наборы политик больше нельзя изменять.
5. Чтобы воспользоваться преимуществами локального хранения, создайте каталог пула хранения для этого пула хранения, используя команду DEFINE STGPOOLDIRECTORY. Дополнительные сведения смотрите в разделе Оптимизация производительности для облачного хранения объектов.

Задачи, связанные с данной:
Подготовка к конфигурированию пулов хранения облачного контейнера для AWS с S3 (не на месте)
Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage с S3 (на месте)
Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage с S3 (не на месте)
Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage со Swift (не на месте)
Подготовка к конфигурированию пулов хранения облачного контейнера для OpenStack со Swift
Шифрование данных для пулов хранения облачных контейнеров
Оптимизация производительности для облачного хранилища объектов
Ссылки, связанные с данной:
SET DBRECOVERY (Задать класс устройств для автоматического резервного копирования)

Подготовка к конфигурированию пулов хранения облачного контейнера для AWS с S3 (не на месте)

Прежде чем конфигурировать пулы хранения облачных контейнеров для использования Amazon Web Services (AWS) вне площадки с использованием протокола Simple Storage Service (S3), нужно получить от Amazon информацию, необходимую для процесса конфигурирования.

Об этой задаче

Идентификационные данные учетной записи AWS отличаются от идентификационных данных учетной записи Amazon. При конфигурировании пулов хранения в компоненте Центр операций или с использованием команды DEFINE STGPOOL используйте идентификационные данные вашей учетной записи AWS.

Для хранения данных AWS использует *участки памяти*. Участки памяти AWS используются так же, как контейнеры в пуле хранения облачных контейнеров. IBM Spectrum Protect автоматически создает в Amazon участок памяти для экземпляра IBM Spectrum Protect, и этот участок памяти совместно используется всеми пулами для этого экземпляра.

Ограничение: Применяются следующие ограничения.

- Измените участок памяти AWS только в IBM Spectrum Protect, не изменяя данные в участке памяти и не изменяя параметры конфигурации для участка памяти.

- В случае пулов хранения облачных контейнеров, которые используют AWS с протоколом Amazon S3, данные по умолчанию шифруются. Однако сервер IBM Spectrum Protect не поддерживает шифрование данных с использованием политик бакетов AWS.

Процедура

1. Войдите в систему, используя учетную запись AWS; для этого перейдите на страницу Amazon S3 и щелкните по Create an AWS Account (Создать учетную запись AWS).
2. Получите свои идентификационные данные AWS:
   a. Перейдите на страницу Amazon S3 и щелкните по Войти на консоль.
   b. Выберите свое имя и выберите Учетные данные защиты.
   c. Перейдите в раздел Ключи доступа, чтобы найти поля ID ключа доступа и Ключ доступа для защиты. Запишите значения, чтобы вы смогли их использовать при конфигурировании пулов хранения.
3. Если вы собираетесь сконфигурировать пулы хранения с помощью мастера Добавить пул хранения в компоненте Центр операций, используйте для параметров команды следующие значения:
   - Тип облака: `Amazon - S3 API`
   - ID ключа доступа: *ID_ключа_доступа*
   - Секретный ключ доступа: *секретный_ключ_доступа*
   - Регион: Выберите конечную точку региона, которая лучше всего подходит к вашему расположению, на основе страницы AWS Regions and Endpoints (Регионы и конечные точки AMS). Если вы выберете `Другой`, задайте URL конечной точки региона в поле URL, включив протокол; как правило, это https://. Обычно для параметра Region можно использовать регион, который находится ближе всего к вашему физическому расположению. Поскольку участок памяти Amazon существует только в одном регионе, вы сможете задать только один URL конечной точки для региона. Если вам требуется регион GovCloud, задайте URL со страницы AWS GovCloud (US) Endpoints (Конечные точки AWS GovCloud (US)).
     Внимание: Используйте в качестве значения региона (Region) только URL конечной точки AWS, например, `https://s3-us-west-1.amazonaws.com`. Не используйте в качестве этого значения статический хостинг-URL веб-сайта.
   - Имя бакета: Используйте имя бакета по умолчанию, сгенерированное сервером, или задайте новое имя бакета.
4. Чтобы задать пул хранения облачного контейнера, введите команду DEFINE STGPOOL со следующими значениями:
   - CLOUDTYPE: S3
   - IDENTITY: *ID_ключа_доступа*
   - PASSWORD: *секретный_ключ_доступа*
   - CLOUDURL: Задайте URL конечной точки региона, который больше всего подходит к вашему расположению, на основе страницы AWS Regions and Endpoints (Регионы и конечные точки AMS Amazon).

     Как правило, для параметра CLOUDURL можно использовать регион, который находится ближе всего к вашему физическому расположению. Если вам требуется регион GovCloud, задайте URL со страницы AWS GovCloud (US) Endpoints (Конечные точки AWS GovCloud (US)).

     Внимание: Используйте в качестве значения CLOUDURL только URL конечной точки AWS, например, `https://s3-us-west-1.amazonaws.com`. Не используйте в качестве этого значения статический хостинг-URL веб-сайта.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера для AWS, следуя инструкциям в разделе Конфигурирование пула хранения облачного контейнера для хранения данных.

Конфигурирование Amazon S3-совместимого устройства в качестве пула хранения облачного контейнера

Вы можете сконфигурировать устройство хранения, совместимое с протоколом Amazon Simple Storage Service (S3), чтобы устройство можно было использовать как пул хранения облачного контейнера IBM Spectrum Protect.

Об этой задаче

Для хранения данных Amazon S3 использует *бакеты* (участки памяти). Вы должны создать бакет на S3-совместимом устройстве для использования сервером IBM Spectrum Protect. После создания бакета используйте учетные данные из

учетной записи на Amazon S3-совместимом облачном устройстве хранения объектов, когда будете конфигурировать пулы хранения с помощью команды DEFINE STGPOOL.

Ограничение: Не изменяя данные в бакете и не изменяйте параметры конфигурации для бакета.

Процедура

1. Создайте бакет на устройстве облачного хранения объектов. Следуйте инструкциям в документации по устройству.
2. Создайте учетную запись пользователя на устройстве облачного хранения объектов. Эта учетная запись используется продуктом IBM Spectrum Protect для доступа к устройству с использованием ID ключа доступа и секретного ключа доступа. Убедитесь, что у учетной записи есть разрешения на хранение данных и удаление данных из бакета, созданного вами в шаге 1. Запишите значения ID ключа доступа и секретного ключа доступа, чтобы вы смогли использовать их при конфигурировании пулов хранения.
3. Узнайте значение URL, которое будет использоваться продуктом IBM Spectrum Protect для доступа к облачному устройству хранения объектов. Инструкции смотрите в документации по вашему облачному устройству хранения объектов.
4. Чтобы задать пул хранения облачного контейнера, введите команду DEFINE STGPOOL со следующими значениями:
   - CLOUDTYPE: S3
   - IDENTITY: *ID_ключа_доступа*
   - PASSWORD: *секретный_ключ_доступа*
   - CLOUDURL: http://*IP_адрес_конечной_точки_облачного_хранилища_объектов* или https://*IP_адрес_конечной_точки_облачного_хранилища_объектов*. Если вы используете более одной конечной точки, перечислите IP-адреса конечных точек, разделяя их вертикальной чертой (|) без пробелов, как показано в следующем примере:

     ```
     CLOUDURL=endpoint_URL1|endpoint_URL2|endpoint_URL3
     ```

   - BUCKETNAME: *имя_бакета_на_устройстве*

     Чтобы оптимизировать производительность, используйте несколько конечных точек или балансировщик нагрузки.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера аналогично тому, как вы бы конфигурировали облачное хранилище объектов IBM Cloud Object Storage, следуя инструкциям в разделе Конфигурирование пула хранения облачного контейнера для хранения данных.

Подготовка к конфигурированию пулов хранения облачного контейнера для Microsoft Azure (не на месте)

Прежде чем конфигурировать пулы хранения облачных контейнеров для использования облачной вычислительной системы Microsoft Azure, нужно получить информацию о процессе конфигурации от Microsoft.

Об этой задаче

IBM Spectrum Protect поддерживает следующие уровни хранения Azure:

- *Горячий уровень хранения* - для данных, доступ к которым осуществляется часто
- *Холодный уровень хранения* - для данных, доступ к которым осуществляется менее часто

Холодный уровень хранения можно использовать для экономичного и долгосрочного хранения. Однако чаще бывает так, что восстановление данных из холодного уровня хранения будет более затратным, чем из горячего уровня хранения.

Процедура

1. Зарегистрируйтесь для получения учетной записи Microsoft Azure, перейдя в портал Azure и создав учетную запись.
2. Создать учетную запись хранения. Как правило, в качестве расположения учетной записи хранения выбирается расположение, самое близкое к вашему серверу IBM Spectrum Protect.
3. Получите свои идентификационные данные Azure:
   a. Перейдите в портал Azure и щелкните по Учетные записи хранения.

b. Откройте новую учетную запись хранения, перейдите в раздел контейнера в панели Служба Blob и запишите значение конечной точки службы blob, чтобы вы смогли использовать его, когда будете конфигурировать пулы хранения. Конечная точка службы blob выглядит как в следующих примерах: https://*имя* .blob.core.windows.net и http://*имя* .blob.core.windows.net.
c. Создайте маркер сигнатуры совместного доступа (shared access signature, SAS), открыв вкладку Сигнатура совместного доступа и заполнив поля. Убедитесь, что в разделе Разрешенные службы указана служба Blob и что в разделе Разрешенные типы ресурсов есть Контейнер и Объект. Убедитесь, что у маркера SAS есть разрешения на чтение, запись, удаление, вызов списка, добавление и создание. Щелкните по Сгенерировать SAS.
d. Запишите значение маркера SAS, чтобы вы смогли использовать его при конфигурировании пулов хранения. IBM Spectrum Protect не отслеживает дату истечения действия маркера SAS, поэтому убедитесь, что вы выбрали дату, наилучшим образом соответствующую вашим требованиям. Если действие маркера закончится, сервер IBM Spectrum Protect утратит доступ к учетной записи хранения, пока вы не предоставите новый маркер SAS.
Совет: Если вы хотели бы менее часть обновлять маркер SAS, задайте срок окончания действия, который не наступит несколько лет. Также убедитесь, что вы проверили поля начальной даты и времени.

4. Если вы собираетесь сконфигурировать пулы хранения с помощью мастера Добавить пул хранения в компоненте Центр операций, используйте для параметров команды следующие значения:
   - Тип облака: `Azure`
   - Маркер SAS: *значение_маркера_SAS*. Ищите строку, аналогичную следующему примеру:

     ```
     ?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:
     12Z&st=2017-04-05T10:26:12Z&spr=https&sig=
     XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
     ```

   - Конечная точка службы Blob: Задайте конечную точку службы Blob из вашей учетной записи Azure, например: https://*имя* .blob.core.windows.net or http://*имя* .blob.core.windows.net.
5. Если вы собираетесь сконфигурировать пулы хранения с помощью команды DEFINE STGPOOL, используйте для параметров команды следующие значения:
   - CLOUDTYPE: Azure
   - PASSWORD: *значение_маркера_SAS*. Ищите строку, аналогичную следующему примеру:

     ```
     ?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:
     12Z&st=2017-04-05T10:26:12Z&spr=https&sig=
     XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
     ```

   - CLOUDURL: Задайте конечную точку службы Blob из вашей учетной записи Azure, например: https://*имя* .blob.core.windows.net or http://*имя* .blob.core.windows.net.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера для Azure, следуя инструкциям в разделе Конфигурирование пула хранения облачного контейнера для хранения данных.

Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage co Swift (не на месте)

Прежде чем конфигурировать пулы хранения облачных контейнеров для использования IBM® Cloud Object Storage и IBM Cloud вне площадки с использованием Swift, нужно получить информацию о конфигурации со страницы IBM Cloud.

Об этой задаче

Когда вы будете конфигурировать пулы хранения с использованием компонента Центр операций или команды DEFINE STGPOOL, используйте идентификационные данные из учетной записи IBM Cloud.

Процедура

1. Создайте учетную запись IBM Cloud, следуя инструкциям в разделе Документация по IBM Cloud.
2. Получите свои идентификационные данные IBM Cloud:
   a. Перейдите на страницу хранения объектов IBM Cloud и войдите в систему, указав идентификационные данные своей учетной записи.
   b. Выберите учетную запись и кластер, которые вы хотите сконфигурировать.

c. В разделе Учетная запись щелкните по Просмотр идентификационных данных
d. В разделе Идентификационные данные учетной записи найдите значения в полях Общедоступная конечная точка аутентификации, Имя пользователя и Ключ API. Запишите значения, содержащиеся в этих полях, чтобы вы смогли их использовать при конфигурировании пулов хранения.

3. Если вы собираетесь сконфигурировать пулы хранения с помощью мастера Добавить пул хранения в компоненте Центр операций, используйте для параметров команды следующие значения:
   - Тип облака: `IBM Cloud Object Storage - Swift API`
   - Имя пользователя: *имя_пользователя*
   - Пароль: *ключ_API*
   - URL: *общедоступная_конечная_точка_аутентификации*
4. Если вы собираетесь сконфигурировать пулы хранения с помощью команды DEFINE STGPOOL, используйте для параметров команды следующие значения:
   - CLOUDTYPE: IBMCLOUDSWIFT
   - IDENTITY: *имя_пользователя*
   - PASSWORD: *ключ_API*
   - CLOUDURL: *общедоступная_конечная_точка_аутентификации*

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера для IBM Cloud, следуя инструкциям в разделеКонфигурирование пула хранения облачного контейнера для хранения данных.

Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage с S3 (не на месте)

Вы можете настроить пулы хранения облачных контейнеров, чтобы работать с IBM® Cloud Object Storage вне площадки с использованием протокола Simple Storage Service (S3).

Об этой задаче

Реализация IBM Cloud Object Storage вне площадки управляется с помощью IBM Cloud. При такой настройке создавать бакеты и администраторов может только владелец учетной записи IBM Cloud.

Когда вы будете конфигурировать пулы хранения с использованием компонента Центр операций или команды DEFINE STGPOOL, используйте идентификационные данные из учетной записи IBM Cloud. Дополнительную информацию смотрите на странице IBM Cloud Storage. Чтобы использовать эту конфигурацию, выберите Облачное хранение объектов - S3 API на странице IBM Cloud Order Object Storage.

Процедура

1. Войдите в портал заказчиков IBM Cloud.
2. Щелкните по меню Хранение и выберите Хранилище объектов.
3. На странице Хранилище объектов выберите учетную запись S3.
4. На странице Облачное хранилище объектов щелкните по Управление бакетами, а затем щелкните по значку +, чтобы создать бакет, который вы хотите использовать с новым пулом хранения облачного контейнера.
5. Щелкните по Показать идентификационные данные, чтобы создать идентификационные данные администратора для вашего нового бакета.
6. Щелкните по Добавить идентификационные данные.
7. Найдите ID ключа доступа:, Секретный ключ доступа: и Общедоступная конечная точка аутентификации. Запишите значения, содержащиеся в этих полях, чтобы вы смогли их использовать при конфигурировании пулов хранения. Если вы находитесь внутри сети IBM Cloud, вы сможете использовать закрытую конечную точку аутентификации.
8. Чтобы сконфигурировать пулы хранения, используя мастер Добавить пул хранения в Центр операций, выберите Облако вне системы. Используйте для параметров следующие значения:
   - Тип облака: `IBM Cloud Object Storage API S3`
   - ID ключа доступа: *ID_ключа_доступа*
   - Секретный ключ доступа: *секретный_ключ_доступа*
   - Имя бакета: *имя_бакета* (из шага 4)
   - URL: *конечная_точка_аутентификации_США_гео*
     Прим.: При такой конфигурации требуется только одна конечная точка провайдера облака. Если все ваши серверы находятся внутри сети IBM Cloud, вы сможете использовать закрытую конечную точку

аутентификации.

9. Если вы конфигурируете пулы хранения с помощью команды DEFINE STGPOOL, то используйте для параметров команды следующие значения:
   - CLOUDTYPE: S3
   - IDENTITY: *ID_ключа_доступа*
   - BUCKETNAME: *имя_бакета* (из шага 4)
   - PASSWORD: *секретный_ключ_доступа*
   - CLOUDURL: *конечная_точка_аутентификации_США_гео*
     Прим.: При такой конфигурации требуется только одна конечная точка провайдера облака. Если все ваши серверы находятся внутри сети IBM Cloud, вы сможете использовать закрытую конечную точку аутентификации.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера для хранилища объектов IBM Cloud, следуя инструкциям в разделеКонфигурирование пула хранения облачного контейнера для хранения данных.

Подготовка к конфигурированию пулов хранения облачного контейнера для IBM Cloud Object Storage с S3 (на месте)

Прежде чем конфигурировать пулы хранения облачных контейнеров для использования IBM® Cloud Object Storage на месте с S3, нужно настроить шаблон хранилища IBM Cloud Object Storage и учетную запись пользователя IBM Cloud Object Storage, а затем получить информацию о конфигурации.

Об этой задаче

Ограничение:

Чтобы использовать IBM Cloud Object Storage на площадке с S3, убедитесь, что ваша версия IBM Cloud Object Storage совместима с версией вашего IBM Spectrum Protect.

При IBM Spectrum Protect версии 8.1.4 IBM Cloud Object Storage требуется V3.8.3 или новее.

Хранилища IBM Cloud Object Storage используются так же, как контейнеры в пуле хранения облачных контейнеров. Настройте шаблон хранилища, чтобы быстро создавать хранилища с использованием ваших предпочтительных параметров.

После создания шаблона хранилища используйте идентификационные данные из своей учетной записи пользователя IBM Cloud Object Storage, чтобы сконфигурировать пулы хранения в Центре операций или команды DEFINE STGPOOL. Сервер использует протокол Simple Storage Service (S3) для взаимодействия с IBM Cloud Object Storage.

Совет: Можно пропустить первые четыре шага в этой процедуре, если требуется сконфигурировать существующее хранилище, используя параметр BUCKETNAME в командах DEFINE STGPOOL или UPDATE STGPOOL.

Процедура

1. Создайте шаблон хранилища:
   a. Войдите в систему IBM Cloud Object Storage и щелкните по вкладке Конфигурировать.
   b. В панели навигации dsNet разверните элемент Пулы хранения.
   c. Выберите пул хранения IBM Cloud Object Storage, в котором вы хотите создать шаблон хранилища, и щелкните по ссылке Пул хранения в разделе Общие.
   d. В разделе Шаблоны хранилищ щелкните по Создать шаблон хранилища.
   e. Выберите параметры для шаблона хранилища по умолчанию. Возможно, вам удастся оптимизировать производительность, не выбирая опции Включить технологию SecureSlice или Индекс имен включен и выбрав опцию Список восстановления включен.
   f. В разделе Внедрение выберите пулы доступа, которые вы хотите использовать для шаблона, и щелкните по Сохранить.
2. Задайте шаблон хранилища как шаблон по умолчанию для IBM Cloud Object Storage dsNet:
   a. Щелкните по вкладке Конфигурировать.
   b. В разделе Конфигурация шаблона хранилища по умолчанию щелкните по Конфигурировать.

c. Выберите шаблон хранилища, который будет использоваться как шаблон по умолчанию, и щелкните по Обновить, чтобы задать этот шаблон как шаблон по умолчанию.

3. Если вы конфигурируете шаблон хранилища впервые, включите роль предоставления хранилищ, которая позволит вам создавать новые хранилища:
   a. Щелкните по вкладке Администрирование.
   b. В разделе Конфигурация API предоставления щелкните по Конфигурировать.
   c. Выберите Только создать или Создать и удалить, чтобы разрешить пользователям создавать новые хранилища при помощи API предоставления.
   d. Нажмите кнопку Обновить, чтобы сохранить параметры.
4. Используйте учетную запись IBM Cloud Object Storage с административными полномочиями, чтобы создать новую учетную запись пользователя в экземпляре IBM Cloud Object Storage в вашей среде. Убедитесь, что у новой учетной записи пользователя есть роль Vault Provisioner (Предоставляющий хранилище).
5. Выберите вкладку Безопасность и выберите новую учетную запись пользователя.
6. Сгенерируйте ключ доступа для нового пользователя:
   a. В разделе Аутентификация ключа доступа щелкните по Изменить ключи.
   b. На странице Изменить ключи доступа щелкните по Сгенерировать ключ доступа.
   c. Нажмите на Назад.
7. В разделе Аутентификация ключа доступа найдите значения ID ключа доступа и Ключ доступа для защиты. Запишите значения, чтобы вы смогли их использовать при конфигурировании пулов хранения.
8. Найдите значение URL:
   a. Щелкните по вкладке Конфигурировать.
   b. В панели навигации dsNet разверните разделы Устройства и Получающий доступ.
   c. Выберите средство доступа к IBM Cloud Object Storage. Проверьте, принадлежит ли получающий доступ к пулу доступа, в котором внедрен шаблон хранилища по умолчанию.
   d. В разделе Конфигурация устройства для получающего доступа запишите значение IP-адрес, чтобы вы смогли его использовать при конфигурировании пулов хранения. Перед значением IP-адреса введите `http://`, чтобы избежать ошибок защиты сертификатов.
9. Если вы конфигурируете пулы хранения с помощью мастера Добавить пул хранения в компоненте Центр операций, используйте для параметров команды следующие значения:
   - Тип облака: `IBM Cloud Object Storage - S3 API`
   - ID ключа доступа: *ID_ключа_доступа*
   - Секретный ключ доступа: *секретный_ключ_доступа*
   - Имя бакета: Используйте имя бакета по умолчанию, сгенерированное сервером, или задайте новое имя бакета.
   - URL: `http://`*IP_адрес_получающего_доступ_к_облачному_складу_объектов*
     Важное замечание: Если у вас более одного получающего доступ, введите IP-адрес получающего доступ, а затем нажмите на Enter, чтобы добавить дополнительные IP-адреса. Чтобы добиться оптимальной производительности, используйте несколько агентов доступа (получающих доступ) или балансировщик нагрузки.
10. Если вы конфигурируете пулы хранения с помощью команды DEFINE STGPOOL, то используйте для параметров команды следующие значения:
    - CLOUDTYPE: S3
    - IDENTITY: *ID_ключа_доступа*
    - PASSWORD: *секретный_ключ_доступа*
    - CLOUDURL: `http://`*IP_адрес_получающего_доступ_к_облачному_складу_объектов*
      Важное замечание: Если вы используете несколько агентов доступа, то перечислите IP-адреса агентов доступа, разделяя их вертикальной чертой (|) без пробелов, например, *CLOUDURL=<URL1_агента_доступа>|<URL2_агента_доступа>|<URL3_агента_доступа>*. Чтобы добиться оптимальной производительности, используйте несколько агентов доступа (получающих доступ) или балансировщик нагрузки.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера для IBM Cloud Object Storage, следуя инструкциям в разделеКонфигурирование пула хранения облачного контейнера для хранения данных.

Подготовка к конфигурированию пулов хранения облачного контейнера для OpenStack co Swift

Прежде чем конфигурировать пулы хранения облачных контейнеров для использования OpenStack co Swift, нужно получить информацию о конфигурации от компьютера OpenStack Swift.

Об этой задаче

Ограничение: Вы должны использовать интерфейс прикладного программирования (application programming interface, API) OpenStack Swift Release Series Juno, главный модуль Service Project, версии 1 или 2.

Когда будете конфигурировать пулы хранения с использованием компонента Центр операций или команды DEFINE STGPOOL, используйте учетные данные из учетной записи OpenStack Swift.

Процедура

1. Создайте учетную запись OpenStack Swift, следуя инструкциям в документации по OpenStack Swift.
2. Получите свои учетные данные OpenStack Swift:
   a. На компьютере OpenStack Swift введите следующую команду:

      ```
      swift auth -v
      ```

   b. Найдите в выходной информации значения `OS_AUTH_URL`, `OS_TENANT_NAME`, `OS_USERNAME` и `OS_PASSWORD`. Запишите значения, чтобы вы смогли их использовать при конфигурировании пулов хранения.
3. Если вы собираетесь сконфигурировать пулы хранения с помощью мастера Добавить пул хранения в компоненте Центр операций, используйте для параметров команды следующие значения:
   - Тип облака: `OpenStack Swift`
   - Имя пользователя: *OS_TENANT_NAME:OS_USERNAME*
   - Пароль: *OS_PASSWORD*
   - URL: *OS_AUTH_URL*
4. Если вы собираетесь сконфигурировать пулы хранения с помощью команды DEFINE STGPOOL, используйте для параметров команды следующие значения:
   - CLOUDTYPE: SWIFT или V1SWIFT
   - IDENTITY: *ИМЯ_АРЕНДАТОРА_ОС:ИМЯ_ПОЛЬЗОВАТЕЛЯ_ОС*
   - PASSWORD: *ПАРОЛЬ_ОС*
   - CLOUDURL: *URL_АВТОРИЗАЦИИ_ОС*
5. Если вы собираетесь использовать определенного арендатора или определенное имя пользователя, запишите значения в следующем формате: *ИМЯ_АРЕНДАТОРА:ИМЯ_ПОЛЬЗОВАТЕЛЯ*.
6. Чтобы не допустить потери данных, сконфигурируйте OpenStack Swift для создания реплик данных, записываемых в соответствующее хранилище объектов. Дополнительную информацию смотрите в документации к OpenStack Swift.

Дальнейшие действия

Сконфигурируйте пулы хранения облачного контейнера, следуя инструкциям в разделе Конфигурирование пула хранения облачного контейнера для хранения данных.

Шифрование данных для пулов хранения облачных контейнеров

Данные, хранящиеся в расположенных вне системы пулах хранения облачных контейнеров, по умолчанию, шифруются. Вы можете дополнительно зашифровать данные в пулах хранения облачных контейнеров на месте.

Об этой задаче

Информацию о шифровании данных пула хранения облачных контейнеров и замечания относительно производительности, связанные с шифрованием данных, смотрите в техническом замечании 1963635.

Как задать правило хранения для уровней облака

Можно задать правило хранения, чтобы реализовать разбиение на облачные слои, при котором данные перемещаются из пула хранения каталога-контейнера на диске в пул хранения облачного контейнера. Правило хранения планирует выделение облачного слоя для перемещения данных из пулов хранения каталогов-контейнеров в пулы хранения облачных контейнеров.

Прежде чем начать

Ограничение: Разбиение на уровни с использованием облака на месте или вне площадки можно сконфигурировать только в облачной вычислительной системе Microsoft Azure или в облачной вычислительной системе с использованием протокола Simple Storage Service (S3).
Учтите следующую информацию:

- Если пул хранения облачного контейнера используется только для операций разбиения на уровни (а не для операций резервного копирования), для пула хранения не требуется локальный каталог хранения (кэш).
- Все экстенты, необходимые для перестройки объекта облака, копируются в уровень, если там еще нет экстентов.
- Если данные сжаты и/или зашифрованы в пуле хранения каталога-контейнера, данные перемещаются в пул хранения облачного контейнера в том же формате.

Об этой задаче

Можно задать правила хранения, чтобы указать следующие требования:

- Время, в течение которого данные остаются в пулах хранения контейнеров на диске, прежде чем будут перемещены в облачное хранилище.
- Является ли правило хранения активным или неактивным. Правила хранения выполняются ежедневно в то время, которое задано в правиле хранения.

Процедура

1. В панели меню компонента Центр операций выберите Хранение > Правила уровней.
2. На странице Правила разбиения хранения на слои щелкните по Создать правило.
3. На странице Создать правило заполните поля и нажмите на Создать.

Результаты

Когда правило хранения активно, сервер определяет, содержат ли исходные пулы каталогов-контейнеров достаточно старые данные, которые нужно переместить. Сервер перемещает данные, подлежащие этой операции, в целевые пулы хранения облачных контейнеров.

Консолидация (высвобождение) пространства в пулах хранения облачных контейнеров

Можно переместить данные из большего, фрагментированного облачного контейнера в меньший, более полно используемый облачный контейнер. Таким образом можно помочь уменьшить стоимость использования хранения объектов для пулов хранения облачных контейнеров.

Прежде чем начать

Ограничения:

- Правило консолидации облака можно сконфигурировать только в облачной вычислительной системе Microsoft Azure или в облачной вычислительной системе с использованием протокола Simple Storage Service (S3).
- Ваш провайдер облачного хранения может взимать плату за перемещение данных, происходящее в результате выполнения операций высвобождения. Перед планированием операций высвобождения пространства используйте Центр операций, чтобы вычислить воздействие, которое могут оказывать разные пороги высвобождения.

Об этой задаче

Когда данные удалены или истек их срок хранения, происходит фрагментация в пулах хранения облачных контейнеров. Чтобы высвободить простанство в пуле хранения облачного контейнера, запланируйте либо ежедневную, либо разовую операцию высвобождения (консолидации) пространства.

Процедура

1. В компоненте Центр операций создайте правило высвобождения пространства, щелкнув по Хранение > Правила.

Либо создайте этот пул, используя команду DEFINE STGRULE с параметром ACTIONTYPE=RECLAIM.

2. Необязательно: Запланируйте специальную операцию по высвобождению (консолидации) пространства, для чего введите команду MOVE CONTAINER с параметром по умолчанию DEFRag=Yes.

Результаты

Когда правило хранения активно, сервер определяет, достиг ли облачный контейнер своего порога для неиспользуемого пространства. Если пространство в контейнере превышает установленный вами порог, экстенты устаревших данных перемещаются в новый, меньший контейнер.

Ссылки, связанные с данной:
DEFINE STGRULE (Задать правило хранения)
DELETE STGRULE (Удалить правила хранения для пулов хранения)
MOVE CONTAINER (Переместить контейнер)
QUERY STGRULE (Показать информацию о правиле хранения)

Оптимизация производительности для облачного хранилища объектов

IBM Spectrum Protect можно сконфигурировать для временного сохранения данных в одном или нескольких каталогах локального пула хранения при поглощении данных. Затем данные перемещаются из локального хранилища в облако. Это позволяет повысить производительность резервного копирования и архивирования данных.

Прежде чем начать

Чтобы оптимизировать производительность резервного копирования и архивирования, убедитесь, что у вас установлен продукт IBM Spectrum Protect версии 8.1.

Об этой задаче

После того как вы зададите каталог пула хранения, сервер IBM Spectrum Protect будет использовать этот каталог как временный целевой пункт для данных, которые вы передается в облачное хранилище объектов. Для передачи данных из локального хранилища в каталоге в облачное хранилище объектов сервер использует автоматизированный фоновый процесс. Для запуска этого процесса переноса или управления им не требуется никаких дополнительных действий. После того как сервер успешно переместить данные из локального хранилища в облачное хранилище объектов, сервер удалит данные из каталога и высвободит пространство для дополнительных поступающих данных.

Если в каталогах пула хранения больше нет свободного пространства, операции резервного копирования преждевременно остановятся. Чтобы этого избежать, можно выделить больше каталогов пула хранения. Также можно дождаться, когда после перемещения данных в облако данные будут автоматически удалены из локальных каталогов. То, какое число каталогов пула хранения вам потребуется задать, зависит от конфигурации дисков на сервере. При первоначальном резервном копировании данных сервер распределяет данные по всем заданным вами каталогам.

Объем пространства, которое вам потребуется для локального хранилища, основан на объеме данных, резервное копирование которых, как вы ожидаете, будет производиться ежедневно после дедупликации и сжатия данных. Если у вас стабильное сетевое соединение с облачным хранилищем объектов, нужный объем пространства будет аналогичен объему, необходимому для ежедневного резервного копирования.

Дополнительную информацию о планировании смотрите в разделе для своей операционной системы:

- AIX: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров
- Linux: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров
- Windows: Планирование для пулов хранения каталогов-контейнеров и пулов хранения облачных контейнеров

Процедура

1. Создайте пул хранения облачного контейнера при помощи мастера Добавить пул хранения в центре операций. Либо создайте этот пул, используя команду DEFINE STGPOOL.
2. Задайте один или несколько каталогов пула хранения, используя команду DEFINE STGPOOLDIRECTORY. Убедитесь, что у каждого каталога пула хранения своя собственная файловая система. В системах Linux используйте в качестве файловой системы xfs или ext4, а не ext3, так как в файловых системах ext3 удаление больших файлов занимает больше времени. Убедитесь, что новые каталоги пула хранения не используют совместно корневую

файловую систему, а также не используют совместно те же файловые системы, которые используются другими ресурсами IBM Spectrum Protect, например, базой данных или журналами.

Ссылки, связанные с данной:
DEFINE STGPOOLDIRECTORY (Задать каталог пула хранения)
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Управление пространством в пулах хранения контейнеров

После того как вы сконфигурируете IBM Spectrum Protect и добавите пространство хранения, вы должны эффективно управлять своими данными и пространством пула хранения, чтобы они правильно функционировали. Используйте пулы хранения контейнеров, чтобы обеспечить максимальное пространство хранения и производительность сервера.

Об этой задаче

Пулы хранения контейнеров - это первичные пулы хранения, которые вы используете для встроенной дедупликации данных, встроенного сжатия и облачного хранения.
Ограничение: Вместе с пулами хранения контейнеров нельзя использовать ни одну из перечисленных ниже функций:

- Перенос
- Освобождение пространства
- Агрегирование
- Совместное размещение
- Экспорт
- Импорт
- Одновременная запись
- Резервное копирование пула хранения
- Виртуальные тома

Процедура

1. Создайте пул хранения каталога-контейнера, сделав следующее:
   a. Откройте Центр операций.
   b. В строке меню компонента Центр операций выберите Хранение > Пулы хранения.
   c. Щелкните по + Пул хранения.
   d. Выполните шаги в мастере Добавить пул хранения:
      - Чтобы использовать встроенную дедупликацию данных, выберите пул хранения Каталог в хранилище на основе контейнеров.
      - При конфигурировании каталогов для пула хранения каталогов-контейнеров задайте пути каталогов, которые вы создали для хранения во время настройки системы.
   e. После того как вы сконфигурируете новый пул хранения каталогов-контейнеров, щелкните по Закрыть и просмотреть политики, чтобы обновить класс управления и начать использовать пул хранения.
2. Чтобы обеспечить оптимальную производительность пулов хранения контейнеров, сделайте следующее:

Задача	Процедура	Дополнительная информация
Защитить пул хранения	При создании пула хранения каталогов-контейнеров в компоненте Центр операций можно сконфигурировать защиту пулов хранения по расписанию, назначенному для пула хранения. Можно также ввести команду PROTECT STGPOOL с исходного сервера, чтобы произвести резервное копирование экстентов данных в пуле хранения каталога-контейнера. Защищая пул хранения, вы не используете ресурсы, которые реплицируют существующие данные	○ Защита данных в пулах хранения каталогов-контейнеров ○ PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения)

	и метаданные, что позволяет повысить производительность сервера.	
Восстановить пул хранения	Если пул хранения защищен, то вы сможете исправить поврежденные экстенты данных командой REPAIR STGPOOL. Используйте команду REPAIR STGPOOL, чтобы исправить пул хранения каталога-контейнера. Ограничение: Если вы реплицируете клиентские узлы, но не защищаете пул хранения каталога-контейнера, вы не сможете исправить пул хранения.	◦ Исправление пулов хранения данных ◦ REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)
Удалить контейнеры	По мере удаления данных файлов или окончании срока их действия контейнеры удаляются из перечня. Используйте команду DEFINE STGPOOL и задайте параметр REUSEDELAY, чтобы управлять тем, в течение какого времени дедуплицированные экстенты будут связаны с пулом хранения каталога-контейнера, после того как ссылок на них больше не будет. Если контейнер поврежден, используйте команду AUDIT CONTAINER, чтобы восстановить или удалить данные.	◦ DEFINE STGPOOL (задать пул хранения каталога-контейнера) ◦ AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации для каталога-контейнера)
Преобазуйте первичный пул хранения, который использует класс устройств FILE, класс ленточных устройств или виртуальную ленточную библиотеку (virtual tape library, VTL)	Существующий пул хранения данных можно преобразовать в пул хранения каталогов-контейнеров, выполнив шаги в разделе Преобразование первичного пула хранения в пул хранения контейнера. Ограничение: Следующие типы пулов хранения преобразовать нельзя: ◦ Первичные пулы хранения, использующие классы устройств с произвольным доступом (DISK) ◦ Пулы хранения копий ◦ Пулы хранения активных данных	◦ CONVERT STGPOOL (преобразовать пул хранения в пул хранения контейнера)
Отслеживайте занятость пула хранения контейнеров	Отслеживайте решение по хранению, чтобы выявить существующие и потенциальные проблемы. Дополнительные сведения смотрите в разделе Мониторинг решений по хранению.	

- Преобразование первичного пула хранения в пул хранения контейнера
  Преобазуйте первичный пул хранения, который использует класс устройств FILE, класс ленточных устройств или виртуальную ленточную библиотеку (virtual tape library, VTL), в пул хранения контейнера. Данные, хранящиеся в пуле хранения контейнеров, могут использовать и встроенную дедупликацию данных, и встроенное сжатие.

- Очистка данных в исходном пуле хранения
  Чтобы преобразовать пул хранения в пул хранения каталогов-контейнеров, нужно стереть поврежденные данные или файлы, которые находятся в исходном пуле хранения.

Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Преобразование первичного пула хранения в пул хранения контейнера

Преобазуйте первичный пул хранения, который использует класс устройств FILE, класс ленточных устройств или виртуальную ленточную библиотеку (virtual tape library, VTL), в пул хранения контейнера. Данные, хранящиеся в пуле хранения контейнеров, могут использовать и встроенную дедупликацию данных, и встроенное сжатие.

Прежде чем начать

Чтобы убедиться, что тома в исходном пуле хранения и связанных пулах хранения копий не используются повторно во время процесса преобразования, задайте значение параметра REUSEDELAY в команде UPDATE STGPOOL. Задайте для параметра REUSEDELAY значение, превышающее длительность преобразования. Вам может потребоваться отложить повторное использование томов по следующим причинам:

- Вы случайно удалили данные во время преобразования пула хранения.
- Вам требуется функция исходного пула хранения, которая недоступна для пулов хранения контейнеров.

Совет: Если вы зададите параметр REUSEDELAY и при этом выполняется операция преобразования, в исходном пуле хранения не будет никакого доступного пространства хранения, пока не истечет время, заданное значением параметра. Создайте пул хранения контейнеров, куда будут перемещаться данные, сделав следующее:

1. На странице Пулы хранения в Центр операций щелкните по + Пул хранения.
2. Выполните шаги в мастере Добавить пул хранения. Выберите нужный вам тип хранения на основе контейнеров.

Об этой задаче

Преобразовав пул хранения в пул хранения контейнера, вы избавитесь от необходимости высвобождения томов. Если пропустить операции высвобождения томов, это может помочь производительность сервера и сократить объем необходимых аппаратных средств.

По мере преобразования файлов все копии, которые хранятся в пулах копий или в пулах активных данных, удаляются. ограничения:

- Если исходный пул указан как резервная копия, архив или назначение переноса для активного набора политик с отложенными изменениями, нужно сначала активировать эти изменения, чтобы преобразовать этот пул.
- Чтобы убедиться, что назначение задает пул хранения, не преобразованный и не подвергающийся преобразованию, вы должны обновить все политики, ссылающиеся на исходный пул хранения.
- Если исходный пул хранения задан как следующий пул хранения, вы должны обновить параметр NEXTSTGPOOL в команде UPDATE STGPOOL, чтобы задать пул хранения со случайным доступом или последовательным доступом, который не подвергается преобразованию.
- Перечисленные ниже типы данных не подлежат преобразованию: резервные копии содержания (table of contents, TOC), виртуальные тома и данные Network Data Management Protocol (NDMP). Прежде чем приступать к процессу преобразования, удалите вручную эти типы данных из пула хранения, переместите типы данных в другой первичный пул хранения или разрешите типам данных истечь в соответствии с параметрами политики.
- При преобразовании пула хранения с классом устройств FILE в пул каталога-контейнера целевой пул хранения должен быть примерно на 30% больше, чем исходный пул хранения. При преобразовании других типов пулов хранения дополнительное пространство, как правило, не требуется.

  Более подробную информацию о наилучших практических методах преобразования пулов хранения смотрите в документе Наилучшие практические методы преобразования пулов хранения IBM Spectrum Protect.

- Если исходный пул хранения используется для сохранения резервных копий TOC, убедитесь, что для сохранения новых резервных копий TOC доступен другой первичный пул хранения. Существующие резервные копии TOC во время преобразования не перемещаются.

Пул TOC должен использовать формат данных NATIVE или NONBLOCK и класс устройств, отличающийся от Centera. Чтобы избежать задержек монтирования, используйте класс устройств DISK или FILE.

Процедура

1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения, использующий класс устройств FILE, класс ленточных устройств или VTL.
2. Выберите Еще > Преобразовать и выполните шаги в мастере Преобразовать пул хранения.
   Совет: Запланируйте преобразование продолжительностью, как минимум, 2 часа для пула хранения, использующего класс устройств FILE, и, как минимум, 4 часа для VTL.

Дальнейшие действия

Когда процесс преобразования завершится, может оказаться, что исходный пул хранения содержит поврежденные данные или данные, несовместимые с пулами хранения контейнеров. Очистите исходный пул хранения, выполнив шаги в разделе Очистка объектов после преобразования пула хранения.

Задачи, связанные с данной:
Восстановление базы данных
 Операционные системы AIX  Операционные системы Linux  Операционные системы Windows

Очистка данных в исходном пуле хранения

Чтобы преобразовать пул хранения в пул хранения каталогов-контейнеров, нужно стереть поврежденные данные или файлы, которые находятся в исходном пуле хранения.

Процедура

Используйте для восстановления или исправления поврежденных данных следующие возможности:

- Восстановите неповрежденную версию данных из пула хранения копий или активных данных, введя команду RESTORE STGPOOL.
- Восстановите неповрежденную версию данных с целевого сервера репликации, введя команду REPLICATE NODE и задав параметр RECOVERDAMAGED=YES.
- Удалите данные, которые после преобразования пула хранения невозможно восстановить, введя команду REMOVE DAMAGED.
  Команда REMOVE DAMAGED не может удалить тома, помеченные в исходном пуле хранения как разрушенные. Чтобы удалить эти тома, сделайте следующее:
  a. Введите команду DELETE VOLUME с параметром DISCARDDATA=YES.
  b. Введите команду CONVERT STGPOOL, чтобы еще раз преобразовать пул хранения.
  c. Если при преобразовании пула хранения будут выявлены поврежденные данные, снова введите команду REMOVE DAMAGED.
- Выполните задачи по анализу, описанные в техническом замечании 1666371.

Дальнейшие действия

После восстановления или исправления поврежденных данных повторите попытку преобразования, введя команду CONVERT STGPOOL.
Чтобы увидеть информацию о поврежденных файлах, оставшихся в исходном пуле хранения, введите команду QUERY CLEANUP.
Совет: Если для пула хранения, в котором нет никаких данных, показано состояние Очистка, можно удалить хранения, используя команду DELETE STGPOOL.
Ссылки, связанные с данной:
DELETE VOLUME (удаление тома пула хранения)
QUERY CLEANUP (Запросить очистку, которая требуется в исходном пуле хранения)
REMOVE DAMAGED (Удалить из исходного пула хранения поврежденные данные)
REPLICATE NODE (Реплицировать данные в файловом пространстве, принадлежащем клиентскому узлу)
RESTORE STGPOOL (восстановление данных в пуле хранения из пула хранения копий или пула активных данных)

Аудит пула хранения

Можно запланировать операции аудита, чтобы идентифицировать запорченные файлы в пулах хранения.

Процедура

Введите команду DEFINE STGRULE с параметром ACTIONTYPE=AUDIT.

Дополнительную информацию о команде DEFINE STGRULE смотрите в разделе DEFINE STGRULE (Задать правило для аудита пулов хранения).

Результаты

Когда правило хранения активно, операции аудита работают согласно заданному расписанию. Информацию о поврежденных файлах можно увидеть, введя команду QUERY DAMAGED.

Если вы обнаружите поврежденные файлы, вы сможете восстановить данные на основе вашей конфигурации. Если вы защитили содержимое пула хранения при помощи команды PROTECT STGPOOL, вы сможете восстановить содержимое пула хранения при помощи команды REPAIR STGPOOL.

Ссылки, связанные с данной:
PROTECT STGPOOL (Защитить данные, принадлежащие к пулу хранения)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения каталогов-контейнеров или в пуле хранения облачных контейнеров)
REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)

Аудит контейнера пула хранения

Произведите аудит пула хранения контейнера, чтобы проверить, нет ли противоречий между информацией в базе данных и в контейнере в пуле хранения.

Об этой задаче

Вы производите аудит пулов хранения контейнеров в следующих случаях:

- При вводе команды QUERY DAMAGED обнаруживается ошибка
- Сервер выводит на экран сообщения о поврежденных экстентах данных
- Ваше оборудование сообщает о проблеме, и появляются сообщения об ошибках, связанные с пулом хранения контейнера

Процедура

1. Чтобы произвести аудит пула хранения на основе контейнеров, введите команду AUDIT CONTAINER. Например, введите следующую команду, чтобы произвести аудит контейнера, 000000000000076c.dcf:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Прочтите выходные данные сообщения ANR4891I, чтобы получить информацию о всех поврежденных экстентах данных.

Дальнейшие действия

При обнаружении проблем с пулом хранения контейнера вы можете восстановить данные на основе вашей конфигурации. Содержимое в пуле хранения можно исправить, используя команду REPAIR STGPOOL.
Ограничение: Содержимое в пуле хранения можно исправить, только если вы защитили пул хранения с использованием команды PROTECT STGPOOL.
Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации о пуле хранения каталога-контейнера)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения каталогов-контейнеров или в облачно-контейнерном пуле хранения)

Требования к системе хранения и уменьшение риска повреждения данных

В случае сервера IBM Spectrum Protect можно использовать много типов хранения. Если вы используете дисковое хранилище блоков, твердотельные накопители (solid-state drive, SSD) или подключенные к сети файловые системы в качестве серверного хранилища, то убедитесь, что хранилище соответствует требованиям.

Для базы данных сервера, активного журнала и архивного журнала, для пулов хранения, использующих классы устройств DISK или FILE, а также для пулов хранения каталогов-контейнеров действуют следующие требования.

Пространство хранения может быть соединено с серверной системой любым способом, который является действительным для операционной системы. Например, пространство хранения может быть подключено непосредственно или с использованием оптоволоконной технологии либо технологии iSCSI.

Поскольку требованиям, предъявляемым серверным хранилищем, может соответствовать много систем хранения, список таких устройств не приводится. Если у вас возникнут вопросы относительного того, соответствует ли система требованиям IBM Spectrum Protect, обращайтесь к поставщику.

Подробную информацию о требованиях файловой системы смотрите в техническом замечании 1902417. Сведения о требованиях сетевых файловых систем (network file system, NFS), смотрите в техническом замечании 1470193.

Системы хранения и файловые системы должны синхронно и точно сообщать на сервер IBM Spectrum Protect о результатах записи и принятия данных. Не сообщенные или сообщенные в асинхронном режиме ошибки записи, приводящие к тому, что данные не принимаются на постоянной основе в систему хранения, могут вызывать повреждение данных. Повреждение данных может вызывать операционные ошибки, включая невозможность запустить сервер, и, как правило, требуется восстановление данных.

Вы можете сократить риск повреждения данных, соблюдая следующие рекомендации:

Кэш записи
: Дисковые системы используют кэш записи, чтобы повысить производительность системы. Чтобы сократить риск повреждения данных, система хранения должна надежным образом принимать данные, находящиеся в кэше записи, в постоянное хранилище.

  Как правило, у кэша записи есть аккумулятор, позволяющий избежать потери данных из кэша во время кратких перебоев с питанием. В случае критически важных систем рассмотрите возможность использовать резервные источники питания, чтобы защитить кэш от длительных перебоев с питанием.

Прямой ввод-вывод
: Прямой ввод-вывод соответствует тому, что серверу требуются синхронные и точные сообщения об операциях записи и принятия данных.
  Внимание: Не выключайте прямой ввод-вывод в ситуациях, когда метод кэширования записи потенциально может вызвать потерю данных. Выключение прямого ввода-вывода может существенно увеличить возможность потери данных, так при этом файловая система будет кэшировать больше данных в дополнение к дисковой системе.

Репликация хранения
: Среды, в которых реплицируется хранилище IBM Spectrum Protect, должны использовать такие функции, как соблюдение порядка записи между источником (локальным сервером) и назначением (удаленным сервером). База данных, активный журнал, архивные журналы и пулы хранения должны быть частью группы согласования. Группа согласования сохраняет взаимосвязи между томами, чтобы сохранить порядок записи, и это позволит их восстановить. Весь ввод-вывод для членов целевой группы согласования должен записываться в том же порядке, как в источнике, и у них должны сохраняться те же характеристики энергонезависимости.

  Чтобы обеспечить синхронизацию между серверами IBM Spectrum Protect на локальном и удаленном сайтах, не запускайте сервер на удаленном сайте за исключением ситуации передачи управления при отказе. Отслеживайте синхронизацию данных в локальном и удаленном расположениях. При потере синхронизации вы должны будете восстановить сервер в удаленном положении, используя команды восстановления IBM Spectrum Protect для базы данных и пулов хранения.

Советы по конфигурированию хранения

Советы по конфигурированию хранения, которые позволят оптимизировать производительность системы, смотрите в перечисленных ниже разделах в документации по продукту V7.1.1. Информацию в контрольных списках можно применить к последующим выпускам.

- Контрольный список для дисков базы данных сервера
- Контрольный список для дисков журнала восстановления сервера
- Контрольный список для пулов хранения, использующих классы устройств DISK или FILE

Мониторинг решений по хранению

После реализации решения IBM Spectrum Protect произведите мониторинг решения, чтобы убедиться, что оно работает правильно. Производя мониторинг решения ежедневно и периодически, можно выявить существующие и потенциальные проблемы. Собранную вами информацию можно использовать, чтобы устранять проблемы и оптимизировать производительность системы.

Об этой задаче

Предпочтительный способ мониторинга решения заключается в использовании компонента Центр операций, который позволяет получить общее и подробное состояние системы в графическом пользовательском интерфейсе. Кроме того, можно сконфигурировать Центр операций для генерирования отчетов по электронной почте, в которых суммируется состояние системы.

Процедура

1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе Контрольный список ежедневного мониторинга.
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе Контрольный список периодического мониторинга.
3. Чтобы проверить, соответствует ли ваша система требованиям по лицензированию, следуйте инструкциям в разделе Проверка соответствия лицензии.
4. Необязательно: Настройте отчеты по электронной почте с информацией о состоянии системы. Инструкции смотрите в разделе Состояние системы отслеживания с использованием отчетов по электронной почте.
5. Необязательно: В некоторых случаях для выполнения отдельных задач по мониторингу или устранению ошибок вам может потребоваться использовать расширенные инструменты мониторинга. Чтобы узнать, как выбрать и сконфигурировать расширенные инструменты мониторинга, смотрите раздел Выбор, конфигурирование и использование инструментов мониторинга.

Дальнейшие действия

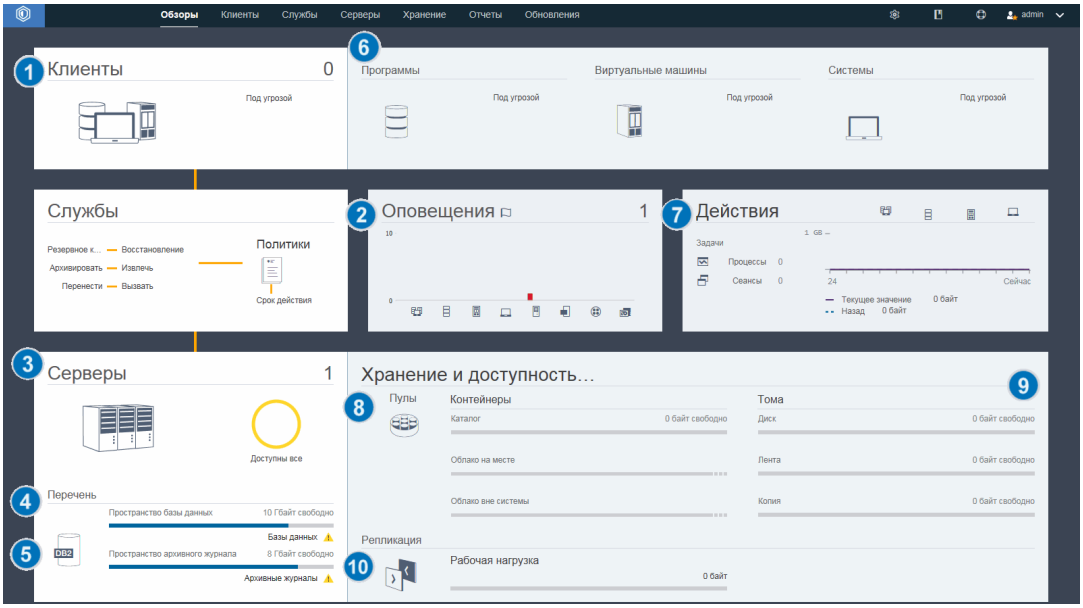
Чтобы помочь вам диагностировать проблемы клиентов резервного копирования и архивирования, установите компонент Службы управления клиентом IBM Spectrum Protect в системах клиента резервного копирования и архивирования, которые его поддерживают. Когда в системе установлен компонент служба управления клиентами, можно щелкнуть в Центр операций по Диагностика, чтобы получить справку по вопросам диагностики для клиента резервного копирования и архивирования. Чтобы установить службу управления клиентом, выполните инструкции в разделе Сбор диагностической информации с использованием Службы управления клиентом IBM Spectrum Protect.
Понятия, связанные с данным:
Производительность
Задачи, связанные с данной:
Диагностика ошибок

Контрольный список ежедневного мониторинга

Ознакомьтесь с контрольным списком, чтобы убедиться, что вы выполняете все задачи по ежедневному мониторингу.

Выполняйте ежедневные задачи мониторинга со страницы Обзор в компоненте Центр операций. Доступ к странице Обзор можно получить, открыв Центр операций и щелкнув по Обзоры.

На рисунке ниже показано расположение для завершения каждой операции.



Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

В следующей таблице перечислены ежедневные задачи мониторинга и представлены инструкции по выполнению каждой задачи.

Табл. 1. Задачи ежедневного мониторинга

Задача	**Основные процедуры**	**Дополнительные процедуры и диагностическая информация**

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
Наблюдайте за уведомлениями о защите, которые могут указывать на атаку программы-вымогателя.	Если потенциальная атака программы-вымогателя обнаружена в среде IBM Spectrum Protect, то будет показано уведомление о защите на переднем плане Центр операций. Дополнительную информацию можно получить, щелкнув по сообщению, чтобы открыть страницу Уведомления о защите.	На странице Уведомления о защите можно выполнить следующие действия: • Просмотр подробностей уведомления по клиентам. Ограничение: В Центр операций версии 8.1.5, уведомления доступны только для клиентов резервного копирования-архивирования. • Подтвердите уведомление защиты, выбрав его и щелкнув по Подтвердить. При подтверждении уведомления о защите в столбец Подтверждение на странице Уведомления о защите добавляется символ галочки для выбранного клиента. Стандарт, по которому подтверждается уведомление, определяется в вашей организации. Галочка может означать, что вы исследовали проблему и решили, что это - ложное положительное. Это также может означать, что проблема существует, и она решается. • Назначьте уведомление о защите администратору, выбрав уведомление о защите и нажав Назначить. Чтобы рассмотреть назначение, администратор должен зарегистрироваться в Центр операций и щелкнуть Обзоры > Защита. Если вы не уверены, что администратор регулярно отслеживает страницу Уведомления о защите, сообщите администратору о назначении. • Если уведомление - ложное положительное, то можно выбрать уведомление о защите и щелкните по Сброс. Уведомление о защите удалено. Хронологические данные, используемые для базовых сравнений с самой последней операцией резервного копирования, удаляются. С этого момента вычисляется новая базовая линия.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
1 Определите, подвергаются ли клиенты риску оказаться незащищенными из-за неудавшихся или пропущенных операций резервного копирования.	Чтобы проверить, находятся ли клиенты под угрозой, в области Клиенты найдите уведомление Под угрозой. Чтобы просмотреть сведения, щелкните по области Клиенты. Внимание: Если процент Под угрозой намного больше обычного, то это может указывать на атаку программы-вымогателя. Атака программы-вымогателя может привести к сбоям резервного копирования, тем самым создавая риск для клиентов. Например, если процент клиентов в опасности обычно между 5% и 10%, но процент увеличивается до 40% или 50%, то изучите причину этого. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете увидеть и проанализировать ошибку клиента и запланировать журналы, выполнив следующие шаги: 1. В таблице Клиенты выберите клиент и щелкните по Сведения. 2. Чтобы диагностировать проблему, щелкните по Диагноз.	В случае клиентов, у которых нет установленной службы управления клиентом, получите доступ к системе клиента, чтобы проверить журналы ошибок клиента.
2 Определите, нужно ли уделить внимание ошибкам клиента или сервера.	Чтобы определить серьезность всех оповещений, о которых было сообщено, установите указатель мыши на столбцы в области Оповещения.	Чтобы увидеть дополнительную информацию об оповещениях, выполните следующие шаги: 1. Щелкните по области Оповещения. 2. В таблице Оповещения выберите оповещение. 3. В панели Журнал операций просмотрите сообщения. В панели показаны связанные сообщения, созданные до и после возникновения выбранного оповещения.
3 Определите, доступны ли серверы, которыми управляет Центр операций, для предоставления клиентам служб по защите данных.	1. Чтобы проверить, находятся ли серверы под угрозой, в области Серверы найдите уведомление Недоступен. 2. Чтобы увидеть дополнительную информацию, щелкните по области Серверы. 3. Выберите сервер в таблице Серверы и щелкните по Сведения.	Совет: Если вы обнаружите проблему, связанную со свойствами сервера, обновите свойства сервера: 1. В таблице Серверы выберите сервер и щелкните по Сведения. 2. Чтобы обновить свойства сервера, щелкните по Свойства.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
4 Определите, доступно ли достаточно пространства для перечня сервера, состоящего из базы данных сервера, активного журнала и архивного журнала.	1. Щелкните по области Серверы. 2. В столбце Состояние в таблице проверьте состояние сервера и устраните все ошибки: ○ Нормальное Для базы данных сервера, активного журнала и архивного журнала доступен достаточный объем пространства. ○ Критическое Для базы данных сервера, активного журнала или архивного журнала недостаточно пространства. Нужно немедленно добавить пространство, иначе работа служб защиты данных, предоставляемых сервером, будет прервана. ○ Предупреждение , В базе данных сервера, активном журнале или архивном журнале заканчивается пространство. Если это условие повторяется, то нужно добавить пространство. ○ Недоступно Невозможно получить состояние. Убедитесь, что сервер работает и что в сети нет ошибок. Это состояние показывается также, если ID администратора мониторинга заблокирован или недоступен на сервере по другой причине. Значение этого ID - IBM-OC-имя_хаб-сервера. ○ Неотслеживаемый Неотслеживаемые серверы заданы на хаб-сервере, но не сконфигурированы для управления компонентом Центр операций. Чтобы сконфигурировать не отслеживаемый сервер, выберите сервер и щелкните по Отслеживать подчиненный.	Можно также просмотреть связанные оповещения на странице Оповещения. Дополнительную информацию об устранении ошибок смотрите в разделе Устранение проблем сервера.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
5 Проверьте операции резервного копирования базы данных.	Чтобы определить, когда в последний раз производилось резервное копирование сервера, выполните следующие шаги: 1. Щелкните по области Серверы. 2. В таблице Серверы проверьте столбец Последнее резервное копирование базы данных.	Чтобы получить более подробную информацию об операциях резервного копирования, выполните следующие шаги: 1. В таблице Серверы выберите строку и щелкните по Сведения. 2. В области Резервное копирование БД установите указатель мыши на галочки, чтобы прочесть информацию об операциях резервного копирования. Если резервное копирование базы данных не производилось недавно (например, за последние 24 часа), вы можете запустить операцию резервного копирования: 1. На странице Обзор в компоненте Центр операций щелкните по области Серверы. 2. В таблице выберите сервер и щелкните по Резервное копирование. Чтобы определить, сконфигурирована ли база данных сервера для автоматических операций резервного копирования, выполните следующие шаги: 1. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY DB: `query db f=d` 3. В выходной информации проверьте значение в поле `Полное имя класса устройств`. Если класс устройства указан, это означает, что сервер сконфигурирован для автоматического резервного копирования базы данных.
6 Отслеживайте другие задачи по обслуживанию сервера. Задачи по обслуживанию сервера могут включать в себя выполнение расписаний административных команд, сценариев обслуживания и связанных команды.	Чтобы найти информацию о процессах, которые завершились неудачно из-за проблем на сервере, выполните следующие шаги: 1. Выберите Серверы > Обслуживание. 2. Чтобы получить двухнедельную хронологию процесса, смотрите столбец Хронология. 3. Чтобы получить больше информации о запланированном процессе, установите указатель мыши на переключателее, связанном с процессом.	Более подробную информацию о процессах мониторинга и устранении проблем смотрите в электронной справке компонента Центр операций.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
7 Убедиться, что объем данных, переданных на серверы и полученных с них, находится в ожидаемом диапазоне.	• Чтобы получить обзор операций за последние 24 часа, смотрите область Операции. • Чтобы сравнить активность за последние 24 часа с активностью за предыдущие 24 часа, смотрите показатели в областях Текущие и Предыдущие.	• Если на сервер было отправлено больше данных, чем вы ожидали, определите, какие клиенты создают резервные копии большего объема данных, и исследуйте причину. Возможно, что дедупликация данных на стороне клиента работает неправильно. Внимание: Если объем резервных данных значительно больше обычного, то это может указывать на атаку программы-вымогателя. Когда программа-вымогатель шифрует данные, система обнаруживает, что данные изменяются и что резервная копия создается для измененных данных. Тем самым тома резервного копирования становятся больше. Чтобы узнать, какие клиенты затронуты, выберите вкладки Приложения, Виртуальные или Системы. • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.
8 Убедитесь, что пулы хранения доступны для резервного копирования данных клиента.	1. Если в области Хранение и доступность данных указаны проблемы, щелкните по Пулы, чтобы ознакомиться со сведениями: ◦ Если показано состояние Критическое ⊗, это указывает на то, что в пуле хранения недостаточно доступного пространства или его состояние доступа - Недоступно. Внимание: Если состояние критическое, то изучите причину: ▪ Если скорость дедупликации данных в пуле хранения значительно снижается, то это может указывать на атаку программы-вымогателя. Во время атаки программы-вымогателя данные шифруются и не могут дедуплицироваться. Чтобы проверить скорость дедупликации данных, в таблице Пулы хранения проверьте значение в столбце Процент экономии. ▪ Если пул хранения неожиданно становится использован 100%, то это может указывать на атаку программы-	Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по Сведения.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
	вымогателя. Для проверки использования просмотрите значение в столбце Использованная емкость. Наведите мышь на значения, чтобы увидеть процент использованного и свободного пространства. ○ Если показано состояние Предупреждение ⚠, в пуле хранения заканчивается пространство или его состояние доступа - Только чтение. 2. Чтобы увидеть и используемое, свободное и общее пространство для выбранного пула хранения, установите указатель мыши над записями в столбце Использованная емкость.	

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
9 Убедитесь, что устройства хранения доступны для операций резервного копирования.	В области Хранение и доступность данных, в разделе Тома под столбцами емкости проверьте состояние, показанное рядом с элементом Устройства. Если для любого устройства показано состояние Критическое или Предупреждение, исследуйте проблему. Чтобы просмотреть сведения, щелкните по Устройства.	Дисковые устройства могут находиться в критическом состоянии или в состоянии предупреждения по следующим причинам: • Для классов устройств DISK тома могут быть отключены или находиться в состоянии 'только для чтения'. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние томов. • Для классов устройств FILE, которые не используются совместно, могут быть отключены каталоги. Кроме того, для выделения чистых томов может оказаться недостаточно свободного пространства. В столбце Дисковое хранение таблицы Дисковые устройства показано состояние каталогов. • Для классов устройств FILE, которые используются совместно, могут быть недоступны накопители. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. В других столбцах таблицы Дисковые устройства показано состояние накопителей и путей. Ленточные устройства могут находиться в состоянии предупреждения или в критическом состоянии, если накопители недоступны. Диск недоступен, если он отключен, перестал отвечать серверу или если его путь отключен. Ленточное устройство может также находиться в критическом состоянии, если библиотека отключена. В других столбцах таблицы Ленточные устройства показано состояние роботизации библиотеки, накопителей и путей. В случае операций резервного копирования лент убедитесь, что доступно достаточное число чистых лент. Если вы не уверены, есть ли у вас достаточное число доступных чистых лент, откройте записную книжку с подробной информацией, чтобы узнать об использовании ленты и увидеть оценку доступности чистых лент. Чтобы открыть записную книжку с подробной информацией, выберите библиотеку в таблице и щелкните по Сведения.

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
10 Отслеживайте процессы репликации узла.	1. Чтобы узнать общее состояние процессов репликации узлов, смотрите область Репликации на странице Обзор в компоненте Центр операций. 2. Чтобы увидеть информацию о каждой паре реплицируемых серверов, щелкните по области Репликация. Внимание: Если вы замечаете неожиданное увеличение числа сбоев при репликации, то это может указывать на атаку программы-вымогателя. Изучите причину сбоев. 3. Чтобы узнать, какой объем данных был реплицирован за последние две недели и какова была скорость репликации, выберите пару серверов и щелкните по Сведения. 4. Чтобы увидеть информацию о репликации для клиента, щелкните по Клиенты на странице Обзор в компоненте Центр операций. Ознакомьтесь с данными в столбце Рабочая нагрузка репликации. Внимание: Если вы замечаете драматическое неожиданное увеличение нагрузки при репликации, то это может указывать на атаку программы-вымогателя. Изучите причину увеличенной нагрузки.	Чтобы выполнить расширенный мониторинг, прочтите информацию о запуске и завершении процессов репликации узлов, используя команды: 1. На странице Обзор компонента Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Введите команду QUERY REPLICATION. Инструкции смотрите в разделе QUERY REPLICATION (Запросить информацию о процессах репликации узлов). Если операция репликации была завершена успешно, значение `Всего файлов, подлежащих репликации` будет соответствовать значению `Всего реплицировано файлов`. Чтобы ознакомиться с сообщениями, связанными с процессом репликации узла на исходном сервере репликации или сервере репликации назначения, выполните следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Серверы. 2. Выберите исходный сервер репликации или сервер репликации назначения и щелкните по Сведения: ○ Чтобы увидеть активные задачи, щелкните по Активные задачи, выберите задачу и проверьте, показано ли состояние Выполняется. Подробные сведения смотрите в соответствующих журналах операций. ○ Чтобы увидеть выполненные задачи, щелкните по Выполненные задачи, выберите задачу и убедитесь, что показано состояние Выполнена. Подробные сведения смотрите в соответствующих журналах операций.

Контрольный список периодического мониторинга

Чтобы убедиться, что операции осуществляются правильно, выполните задачи в периодическом контрольном списке мониторинга. Запланируйте периодические задачи достаточно часто, чтобы вы могли обнаружить потенциальные неполадки, прежде чем они вызовут проблемы.

Совет: Чтобы выполнять команды администрирования для дополнительных задач по мониторингу, используйте построитель команд компонента Центр операций. Построитель команд обеспечивает функцию ввода с опережением, которая поможет по мере ввода команд. Чтобы открыть построитель команд, перейдите на страницу Обзор в компоненте Центр операций. В строке меню установите указатель мыши на значок параметров и щелкните по Построитель команд.

Табл. 1. Задачи периодического мониторинга

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте производительность системы.	Определите, сколько времени требуется для операций резервного копирования клиента: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. Найдите сервер, связанный с клиентом. 2. Щелкните по Серверы. Выберите сервер и щелкните по Сведения. 3. Чтобы увидеть продолжительность выполненных задач за последние 24 часа, щелкните по Выполненные задачи. 4. Чтобы увидеть продолжительность задач, выполненных более 24 часов тому назад, используйте команду QUERY ACTLOG. Следуйте инструкциям в разделе . 5. Если длительность операций резервного копирования клиента увеличивается при неясных причинах, исследуйте причину. Если вы установили службу управления клиентом на клиенте резервного копирования и архивирования, вы сможете диагностировать ошибки, влияющие на производительность, для клиента резервного копирования и архивирования, выполнив следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты. 2. Выберите клиент резервного копирования и архивирования и щелкните по Сведения. 3. Чтобы получить журналы клиентов, щелкните по Диагностика.	Инструкции по сокращению времени, которое затрачивает клиент на резервное копирование данных на сервер, смотрите в разделе Устранение общих проблем, связанных с производительностью клиента. Ищите узкие места с точки зрения производительности. Инструкции смотрите в разделе Выявление узких мест производительности. Информацию о выявлении и устранении других проблем, отрицательно влияющих на производительность, смотрите в разделе Производительность.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите экономию дисков, обеспечиваемую дедупликацией данных.	1. Щелкните на странице Обзор в компоненте Центр операций по Пулы. 2. Выберите пул щелкните по Быстрый обзор. 3. В области Дедупликация данных смотрите сохраненную строку Пространство.	При расширенном мониторинге, чтобы получить подробную статистику процесса дедупликации данных для определенного пула хранения контейнеров каталогов или облачного пула хранения каталогов, выполните следующие шаги: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Получите статистический отчет, введя команду GENERATE DEDUPSTATS. Следуйте инструкциям в разделе GENERATE DEDUPSTATS (Сгенерировать статистику дедупликации данных для пула хранения каталога-контейнера). 3. Просмотрите статистический отчет, введя команду QUERY DEDUPSTATS. Следуйте инструкциям в разделе QUERY DEDUPSTATS (Запросить статистику дедупликации данных).

Убедитесь, что текущие файлы резервных копий для конфигурации устройств и информации о хронологии томов сохранены.	Получите доступ к расположениям хранения, чтобы убедиться, что файлы доступны. Предпочтительный метод заключается в том, чтобы сохранять файлы резервных копий в двум расположениях.
	Чтобы найти файлы хронологии томов и файлы конфигурации устройств, выполните следующие шаги:
	1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд.
	2. Чтобы найти файлы хронологии томов и конфигурации устройств, введите следующие команды:
	`query option volhistory`
	`query option devconfig`
	3. В выходной информации проверьте столбец Параметр опции, чтобы найти расположения файлов.
	Если произойдет бедствие, для восстановления базы данных сервера потребуется как файл хронологии томов, так и файл конфигурации устройств.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Определите, доступно ли достаточно пространства для файловой системы каталога экземпляра.	Убедитесь, что в файловой системе каталога экземпляра доступно, как минимум, 20% свободного пространства. Выполните действие, подходящее для вашей операционной системы: •  Операционные системы AIX Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -g` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Linux Чтобы увидеть, сколько пространства доступно в файловой системе, введите в командной строке операционной системы следующую команду: `df -h` *`каталог_экземпляра`* где *каталог_экземпляра* - это каталог экземпляра.  Операционные системы Windows В проводнике Windows щелкните правой кнопкой мыши по файловой системе и выберите Свойства. Проверьте информацию о емкости. Предпочтительное расположение каталога экземпляра зависит от операционной системы, в которой установлен сервер: •  Операционные системы AIX  Операционные системы Linux /home/tsminst1/tsminst1  Операционные системы Windows C:\tsminst1 Совет: Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.	

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Выявите неожиданную активность клиента.	Чтобы отслеживать операции клиента и определить, не превышает ли объем данных для томов ожидаемый объем, выполните следующие шаги: 1. На странице Обзор в компоненте Центр операций щелкните по области Клиенты. 2. Чтобы увидеть операции за посредние две недели, дважды щелкните по любому клиенту. 3. Чтобы узнать число байт, отправленных клиенту, щелкните по вкладке Свойства. 4. В области Последний сеанс проверьте строку Отправлено клиенту.	Когда вы дважды щелкнете по клиенту в таблице Клиенты, в области Операции за 2 недели будет показан объем данных, которые клиент каждый день отправлял на сервер. Регулярно проверяйте SQL-таблицу сводной информации о деятельности, содержащую статистические данные о клиентских сеансах. Чтобы сравнить текущие операции с предыдущими, воспользуйтесь оператором SQL SELECT. Если уровень операций существенно отличается от предыдущего, то это может указывать на атаку программы-вымогателя. Регулярно проверяйте журнал операций. Найдите сообщения ANE, указывающие, для скольких файлов созданы резервные копии и выполнена инспекция. Сравните текущие данные о скорости дедупликации с прежней скоростью. Если в созданной резервной копии необычно много файлов или уровень дедупликации данных неожиданно спадает до 0, то это может указывать на атаку программы-вымогателя

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Отслеживайте рост пула хранения с течением времени.	1. На странице Обзор в компоненте Центр операций щелкните по области Пулы. 2. Чтобы увидеть емкость, используемую за последние две недели, выберите пул и щелкните по Сведения.	Советы: • Чтобы задать период времени, который должен пройти, прежде чем из пула хранения каталогов-контейнеров или пула хранения облачных контейнеров будут удалены все дедуплицированные экстенты, после того как на них не появлялось никаких ссылок в перечне, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. 3. Задайте длительность в поле `Период задержки для повторного использования контейнера`. • Чтобы определить производительность дедупликации данных для пулов хранения каталогов-контейнеров и облачных контейнеров, используйте команду GENERATE DEDUPSTATS. • Чтобы просмотреть статистику дедупликации данных для пула хранения, выполните следующие шаги: 1. На странице Пулы хранения в компоненте Центр операций выберите пул хранения. 2. Выберите Сведения > Свойства. Либо используйте команду QUERY EXTENTUPDATES, чтобы увидеть информацию об обновлениях экстентов данных в пулах хранения каталогов-контейнеров или облачных контейнеров. Выходная информация команды может помочь вам определить, на какие экстенты данных уже нет ссылок и какие из них подлежат удалению из системы. В выходной информации смотрите, какое число экстентов данных подлежит удалению из системы. Этот показатель напрямую коррелируется с объемом свободного пространства, которое будет доступно в пуле хранения контейнера. • Чтобы увидеть объем физического пространства, занятого файловым пространством после удаления экономии за счет дедупликации данных, используйте команду select * from occupancy. В выходной информации команды будет содержаться значение LOGICAL_MB. LOGICAL_MB - это объем, используемый этим файловым пространством.

Задача	Основные процедуры	Дополнительные процедуры и устранение ошибок
Оцените временные характеристики расписаний клиента. Убедитесь, что начальное и конечное время расписаний клиентов соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Клиенты > Расписания. В таблице Расписания в столбце Запуск показано сконфигурированное время запуска для запланированной операции. Чтобы увидеть, когда была запущена самая последняя операция, установите указатель мыши на значок часов.	Совет: Если операция клиента выполняется дольше, чем ожидается, вы можете получить сообщение с предупреждением. Сделайте следующее: 1. На странице обзора в компоненте Центр операций установите указатель мыши на Клиенты и щелкните по Расписания. 2. Выберите расписание и щелкните по Сведения. 3. Просмотрите сведения о расписании, щелкнув по синей стрелке рядом со строкой. 4. В поле Оповещение среды выполнения задайте время, когда будет выдано сообщение с предупреждением, если запланированная операция не будет выполнена. 5. Щелкните по Сохранить.
Оцените временные характеристики задач по обслуживанию. Убедитесь, что начальное и конечное время задач по обслуживанию соответствует вашим бизнес-требованиям.	Щелкните на странице Обзор в компоненте Центр операций по Серверы > Обслуживание. В таблице Обслуживание проверьте информацию в столбце Время последнего выполнения. Чтобы увидеть, когда была запущена самая последняя задача по обслуживанию, установите указатель мыши на значок часов.	Совет: Если задача по обслуживанию выполняется слишком долго, измените начальное время или максимальное время выполнения. Сделайте следующее: 1. На странице Обзор Центр операций установите указатель мыши на значок параметров и щелкните по Построитель команд. 2. Чтобы изменить время запуска или максимальное время выполнения задачи, введите команду UPDATE SCHEDULE. Инструкции смотрите в разделе UPDATE SCHEDULE (Изменить запланированное задание клиента).

Ссылки, связанные с данной:
UPDATE STGPOOL (обновить пул хранения)
QUERY EXTENTUPDATES (Запросить обновленные экстенты данных)

Проверка на соответствие лицензии

Убедитесь, что ваше решение IBM Spectrum Protect соответствует положениям вашего лицензионного соглашения. Регулярно производя мониторинг решения, можно отслеживать тенденции роста данных или использование единиц мощности процессора (processor value unit, PVU). Используйте эту информацию, чтобы спланировать будущее приобретение лицензий.

Об этой задаче

Метод, который вы используете, чтобы убедиться, что ваше решение соответствует условиям лицензии, зависит от положений вашего лицензионного соглашения IBM Spectrum Protect.

Фронтальное лицензирование мощности
: Фронтальная модель определяет требования к лицензии на основе объема первичных данных, о которых клиентами было сообщено, что для них создавались резервные копии. К клиентам относятся приложения, виртуальные машины и компьютеры.

Внутреннее лицензирование мощности

Внутренняя модель определяет требования к лицензии на основе числа терабайт данных, которые хранятся в первичных пулах хранения и репозиториях.
Советы:

- Чтобы обеспечить точность оценки фронтальной и внутренней емкости, установите новейшую версию программы клиента на каждом клиентском узле.
- Информация о фронтальной и внутренней емкости в Центр операций предназначена только для планирования и оценки.

Лицензирование PVU

Модель PVU основана на использовании PVU серверными устройствами.
Важное замечание: Расчеты PVU, выполняемые IBM Spectrum Protect, считаются оценочными и не имеют юридической силы. Информация о лицензировании PVU, сообщенная продуктом IBM Spectrum Protect, не рассматривается как допустимая замена для IBM® License Metric Tool.

Самую последнюю информацию о моделях лицензирования смотрите в информации о продукте и лицензии на веб-сайте семейства продуктов IBM Spectrum Protect. Если у вас возникнут вопросы или замечания, касающиеся требований по лицензированию, обращайтесь к вашему поставщику программы IBM Spectrum Protect.

Процедура

Чтобы отследить соответствие лицензии, выполните шаги, соответствующие положениям вашего лицензионного соглашения.
Совет: Центр операций обеспечивает электронный отчет, в котором просуммировано использование фронтальной и внутренней емкости. Отчеты можно автоматически регулярно отправлять одному или нескольким получателям. Чтобы сконфигурировать электронные отчеты и управлять ими, щелкните по Отчеты в строке меню Центр операций.

Опция	Описание
Фронтальная модель	a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. На странице Фронтальное использование показана оценка фронтальной емкости. b. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости. c. Чтобы оценить емкость для клиентов, которые не сообщают об использовании емкости, перейдите на следующий FTP-сайт, где представлены инструменты измерения и инструкции: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Чтобы изменить фронтальную емкость в соответствии со сценарием, выполните инструкции в самом последнем доступном руководстве по лицензированию. d. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария. e. Убедитесь, что оценка емкости соответствует вашему лицензионному соглашению.
Внутренняя модель	Ограничение: Если исходный и целевой серверы репликации не используют одни и те же параметры политики, вы не сможете использовать Центр операций для мониторинга использования внутренней емкости для реплицируемых клиентов. Информацию о том, как оценить использование емкости для этих клиентов, смотрите в следующей публикации technote 1656476. a. В строке меню компонента Центр операций установите указатель мыши на значок параметров и щелкните по Лицензирование. b. Щелкните по вкладке Внутренний. c. Проверьте, соответствует ли оценка объема данных вашему лицензионному соглашению.
Модель PVU	Иформацию о том, как оценить соответствие условиям лицензирования PVU, смотрите в разделе Оценка соответствия модели лицензирования PVU.

- Оценка соответствия модели лицензирования PVU
  Если вы приобрели IBM Spectrum Protect в соответствии с моделью лицензирования на основе эффективных единиц процессора (processor value unit, PVU), убедитесь, что ваше решение соответствует положениям лицензии. Периодически знакомьтесь с оценками PVU, чтобы спланировать будущую покупку лицензии. Например, если оценки PVU возрастают или вы планируете установить больше серверов, вам, возможно, придется приобрести больше лицензий.

Состояние системы отслеживания с использованием отчетов по электронной почте

Настройте компонент Центр операций, чтобы сгенерировать отчеты по электронной почте, в которых суммируется состояние системы. Вы можете сконфигурировать соединение с почтовым сервером, изменить параметры отчета и (необязательно) создать пользовательские отчеты.

Прежде чем начать

Прежде чем настраивать отчеты по электронной почте, убедитесь, что выполнены следующие требования:

- Доступен хост-сервер Simple Mail Transfer Protocol (SMTP) для отправки и получения отчетов по электронной почте. Сервер SMTP должен быть сконфигурирован как открытый почтовый ретранслятор. Вы также должны убедиться, что у сервера IBM Spectrum Protect, который отправляет сообщения электронной почты, есть доступ к серверу SMTP. Если центр операций установлен на отдельном компьютере, этому компьютеру не требуется доступ к серверу SMTP.
- Чтобы задавать отчеты по электронной почте, нужно иметь системные полномочия для сервера.
- Чтобы задать получателей, можно ввести один или несколько адресов электронной почты или ID администраторов. Если вы собираетесь ввести ID администратора, ID должен быть зарегистрирован на хаб-сервере и с ним должен быть связан адрес электронной почты. Чтобы задать адрес электронной почты для администратора, используйте параметр EMAILADDRESS в команде UPDATE ADMIN.

Об этой задаче

Вы можете сконфигурировать Центр операций для отправки отчета об общих операциях, отчета о соответствии лицензии, а также одного или нескольких пользовательских отчетов. Вы создаете пользовательские отчеты, выбирая шаблоны из набора обычно используемых шаблонов отчетов или вводя операторы SQL SELECT, чтобы запросить информацию на управляемых серверах.

Процедура

Чтобы настроить электронные отчеты и управлять ими, сделайте следующее:

1. В строке меню компонента Центр операций выберите Отчеты.
2. Если соединение с сервером электронной почты еще не сконфигурировано, щелкните по Сконфигурировать почтовый сервер и заполните поля. После того как вы сконфигурируете почтовый сервер, будут включены отчет об общих операциях и отчет о соответствии лицензии.
3. Чтобы изменить параметры отчета, выберите отчет, щелкните по Сведения и обновите форму.
4. Необязательно: Чтобы добавить пользовательский отчет, щелкните по + Отчет и заполните поля.
   Совет: Чтобы сразу же запустить и отправить отчет, выберите отчет и нажмите на Отправить.

Результаты

Разрешенные отчеты будут отправлены в соответствии с заданными параметрами.
Ссылки, связанные с данной:
UPDATE ADMIN (обновление администратора)
Информация, связанная с данной:
Примеры пользовательских отчетов

Выбор, конфигурирование и использование инструментов мониторинга

Используйте Центр операций, чтобы получить обзор состояния системы и получить возможность раскрыть более подробную информацию. В некоторых случаях для сбора определенной информации мониторинга может потребоваться использовать расширенные инструменты.

Процедура

Выберите и сконфигурируйте инструменты мониторинга, подходящие для вашего решения.

Табл. 1. Инструменты мониторинга

Тип инструмента	Случаи использования	Ссылки на дополнительную информацию
Центр операций	• Используйте графический пользовательский интерфейс, чтобы проверить состояние системы и диагностировать проблемы. • Настройте Центр операций для отправки ежедневных сводных отчетов по электронной почте. • (Необязательно) Настройте оповещения, появляющиеся в компоненте Центр операций, и настройте уведомления с оповещениями, отправляемые по электронной почте. • Необязательно: Произведите дистанционный мониторинг среды хранения, просматривая страницу Обзор в веб-браузере мобильного устройства. Например, на устройстве Apple iPad можно использовать веб-браузер Apple Safari. Можно использовать и другие мобильные устройства. Совет: При установке службы управления клиентом на клиенте резервного копирования и архивирования можно использовать компонент Центр операций, чтобы получить информацию по устранению ошибок клиента резервного копирования и архивирования. Службу управления клиентом можно установить только в операционных системах Linux или Windows.	

Тип инструмента	Случаи использования	Ссылки на дополнительную информацию
Команды администрирования IBM Spectrum Protect	Проверьте подробную информацию. Используйте метод, подходящий для вашего решения. • Чтобы увидеть сообщения, сгенерированные для сервера и клиента, используйте команду QUERY ACTLOG. Совет: Административные команды можно запускать из построителя команд в компоненте Центр операций. • Чтобы отслеживать такие действия, как перенастройку сервера и входы клиентов в систему, используйте клиент администрирования в режиме консоли. Введите команду dsmadmc -consolemode.	• Административные команды • QUERY ACTLOG (Запросить информацию журнала операций) • Наблюдение за работой сервера через клиент администрирования • Опции клиента администрирования
Запись событий в журнал ошибок	Записывайте сообщения сервера и большинство сообщений клиента в виде событий в один или несколько репозиториев, которые называются приемниками.	Операционные системы AIX Операционные системы Linux Операционные системы WindowsИнструкций об использовании записи событий в журнал для мониторинга решения смотрите в разделе Запись событий IBM Spectrum Protect в приемники (V7.1.1). Операционные системы LinuxИнструкции по записи событий в системный журнал Linux смотрите в разделе Запись событий в системный журнал Linux (V7.1.4).
Запросы SQL	Создайте и сформатируйте настроенные запросы для базы данных сервера. Например, можно запросить информацию из сводной таблицы операций SQL, чтобы увидеть статистику операций клиентов и серверных процессов. Чтобы увидеть всю информацию в сводной таблице, введите на клиенте администрирования следующую команду: `select * from summary`	Использование команд SELECT (V7.1.1)
Инструменты операционной системы	Отслеживайте и проверяйте производительность системы.	

Тип инструмента	Случаи использования	Ссылки на дополнительную информацию
Инструменты мониторинга устройств	Отслеживайте доступность, емкость и производительность устройств. Например, используйте IBM Spectrum Control или инструменты, прилагаемые к пакетам оборудования устройств.	Чтобы отслеживать общее состояние устройств с использованием IBM Spectrum Control, следуйте инструкциям в разделе Мониторинг состояния и условий ресурсов. Чтобы отслеживать производительность с использованием IBM Spectrum Control, следуйте инструкциям в разделе Мониторинг производительности ресурсов.
IBM® Tivoli Monitoring for Tivoli Storage Manager	Отслеживайте серверы IBM Spectrum Protect и создавайте хронологические отчеты об операциях сервера и клиента. Совет: Компонент Центр операций - это предпочтительный инструмент мониторинга. Однако компонент Tivoli Monitoring for Tivoli Storage Manager полезен для генерирования хронологических отчетов на основе технологии IBM Cognos Business Intelligence.	Tivoli Monitoring for Tivoli Storage Manager

Управление операциями

Эффективно управляя операциями сервера и клиента, вы сможете оптимизировать производительность среды хранения. Чтобы приступить к работе, произведите мониторинг среды, используя компонент Центр операций. Затем выполните соответствующие действия, чтобы избежать потенциальных проблем и повысить производительность.

Об этой задаче

- Управление операциями сервера
  Можно останавливать и запускать сервер, управлять емкостью перечня и управлять использованием памяти и процессора. Вы можете также оптимизировать передачу данных между серверами, обновлять сервер и настраивать запланированные действия.
- Управление операциями клиентов
  Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.
- Управление Центром операций
  Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.

Управление операциями сервера

Можно останавливать и запускать сервер, управлять емкостью перечня и управлять использованием памяти и процессора. Вы можете также оптимизировать передачу данных между серверами, обновлять сервер и настраивать запланированные действия.

- Остановка и запуск сервера
  Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.
- Управление емкостью перечня
  Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

- Управление использованием памяти и процессора
  Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.
- Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде
  Если ваш сервер IBM Spectrum Protect реплицирует узлы или защищает пулы хранения на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Прежде чем включить технологию Aspera FASP, вы должны получить соответствующие лицензии. Доступна как лицензия на оценку, так и полная лицензия.
- Планирование обновления сервера
  Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.
- Тонкая настройка запланированных операций
  Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Остановка и запуск сервера

Прежде чем выполнять задачи по обслуживанию или переконфигурированию, остановите сервер. Затем запустите сервер в режиме обслуживания. Когда завершите задачи по обслуживанию или переконфигурированию, перезапустите сервер в производственном режиме.

Прежде чем начать

Чтобы остановить и запустить сервер IBM Spectrum Protect, требуются системные полномочия или полномочия оператора.

- Остановка сервера
  Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.
- Запуск сервера для задач обслуживания или реконфигурирования
  Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Остановка сервера

Прежде чем остановить сервер, подготовьте систему, проследив, чтобы все операции по резервному копированию базы данных были завершены и чтобы все прочие процессы и сеансы были закончены. Благодаря этому, вы сможете безопасным образом завершить работу сервера и обеспечить защиту данных.

Об этой задаче

При вводе команды HALT для остановки сервера происходят следующие действия:

- Все процессы и сеансы узлов клиентов будут отменены.
- Все текущие транзакции будут остановлены. (При перезапуске сервера будет произведен откат транзакций.)

Процедура

Чтобы подготовить систему и остановить сервер, выполните следующие шаги:

1. Запретите запуск новых сеансов клиентских узлов, введя команду DISABLE SESSIONS:

   ```
   disable sessions all
   ```

2. Определите, не выполняются ли какие-либо сеансы клиентских узлов или процессы, выполнив следующее:

a. На странице Центра операций Обзор посмотрите в области Активность общее число процессов и сеансов, которые активны в настоящий момент. Если это число заметно отличается от значения, которое обычно показано во время повседневного управления хранением, то просмотрите другие индикаторы состояния в Центре операций, чтобы определить, ошибка ли это.
b. Смотрите график в области Активность, чтобы сравнить объем сетевого трафика за следующие периоды:
   - Текущий период, то есть, самые последние 24 часа
   - Предыдущий период, то есть, за 24 часа до текущего периода

   Если на графике за предыдущий период показано ожидаемый объем трафика, существенные различия с графиком за текущий период могут указывать на проблему.
c. Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения. Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, получите информацию о процессах при помощи команд администрирования. Введите команду QUERY PROCESS для запроса процессов и получения информации о сеансах при помощи команды QUERY SESSION.

3. Дождитесь завершения сеансов клиентских узлов или отмените их. Чтобы отменить процессы и сеансы, сделайте следующее:
   - Выберите на странице Серверы сервер, для которого вы хотите посмотреть процессы и сеансы, и щелкните по Сведения.
   - Щелкните по вкладке Активные задачи и выберите один или несколько процессов, сеансов или комбинацию процессов и сеансов, которые вы хотите отменить.
   - Нажмите кнопку Отмена.
   - Если сервер не зарегистрирован как хаб или подчиненный сервер в Центр операций, отмените сеансы при помощи команд администрирования. Введите команду CANCEL SESSION, чтобы отменить сеанс и процессы при помощи команды CANCEL PROCESS.
     Совет: Если процесс, который вы хотите отменить, ожидает монтирования ленточного тома, требование монтирования будет отменено. Например, если вы введете команду EXPORT, IMPORT или MOVE DATA, команда может инициировать процесс, для которого потребуется смонтировать ленточный том. Однако, если ленточный том монтируется автоматизированной библиотекой, операция отмены может не иметь силы, пока не завершится процесс монтирования. В зависимости от вашей системной среды на это может потребоваться несколько минут.
4. Остановите сервер с помощью команды HALT:

```
halt
```

Запуск сервера для задач обслуживания или реконфигурирования

Прежде чем приступить к выполнению задач по обслуживанию или переконфигурированию, запустите сервер в режиме обслуживания. При запуске сервера в режиме обслуживания вы отключаете операции, которые могут помешать задачам обслуживания или переконфигурирования.

Об этой задаче

Запустите сервер в режиме обслуживания, запустив утилиту DSMSERV с параметром MAINTENANCE.

В режиме обслуживания отключаются следующие операции:

- Расписания выполнения административных команд
- Клиентские расписания
- Восстановление пространства хранения на сервере
- Устаревание инвентарного перечня
- Перенастройка пулов хранения

Кроме того, клиентам запрещено запускать сеансы с сервера.
Советы:

- Чтобы запустить сервер в режиме обслуживания, не нужно изменять файл опций сервера, dsmserv.opt.
- Когда сервер работает в режиме обслуживания, вы можете вручную запустить восстановление пространства хранения, истечение срока действия перечня и процессы переноса пулов хранения.

Процедура

Чтобы запустить сервер в режиме обслуживания, введите следующую команду:

```
dsmserv maintenance
```

Совет: Видеоклип, иллюстрирующий запуск сервера в режиме обслуживания, смотрите на веб-странице Запуск сервера в режиме обслуживания.

Дальнейшие действия

Чтобы возобновить операции сервера в производственном режиме, выполните следующие шаги:

1. Завершите работу сервера с помощью команды HALT:

   ```
   halt
   ```

2. Запустите сервер, используя метод, который вы используете в производственном режиме. Выполните инструкции для вашей операционной системы.
   - Операционные системы AIXЗапуск экземпляра сервера
   - Операционные системы LinuxЗапуск экземпляра сервера
   - Операционные системы WindowsЗапуск экземпляра сервера

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Управление емкостью перечня

Управляйте емкостью базы данных, активного журнала и архивных журналов, чтобы размер перечня определялся для задач на основе состоянии журналов.

Прежде чем начать

У активного и архивного журналов есть следующие особенности:

- Максимальный размер активного журнала равен 512 ГБ. Более подробную информацию о размерах активного журнала для вашей системы смотрите в разделе Планирование массивов хранения.
- Размер архивного журнала ограничен размером файловой системы, в которой он установлен. Размер архивного журнала не поддерживается на заранее заданном уровне, как в случае активного журнала. Архивные файлы журналов автоматически удаляются, когда они становятся больше не нужны.

(Необязательно) Лучше всего создать архивный журнал отказоустойчивости, чтобы сохранять файлы архивного журнала при переполнении каталога архивных журналов.

Проверьте Центр операций, чтобы определить, какой компонент перечня переполняется. Прежде чем увеличивать размер одного из компонентов перечня, убедитесь, чтобы вы остановили сервер.

Процедура

- Чтобы увеличить размер базы данных, выполните следующие шаги:
  - Создайте один или несколько каталогов для базы данных на отдельных накопителях или в файловых системах.
  - Введите команду EXTEND DBSPACE, чтобы добавить каталог или каталоги к базе данных. Каталоги должны быть доступны для ID пользователя экземпляра менеджера базы данных. По умолчанию данные перераспределяются по всем каталогам базы данных и пространство высвобождается.
    Советы:
    - Время, необходимое для полного перераспределения данных и высвобождения пространства, изменяется в зависимости от размера вашей базы данных. Убедитесь, что это учтено при планировании.
    - Убедитесь, что размер указанных каталогов совпадает с размером существующих каталогов, чтобы обеспечить согласованную степень параллелизма для операций базы данных. Если один или более каталогов для базы данных окажутся меньше других, это уменьшит оптимизированное параллельное упреждающее чтение и распределение базы данных.
  - Остановите и перезапустите сервер для полного использования новых каталогов.
  - Если потребуется, исправьте базу данных. Реорганизация индекса и таблиц для базы данных сервера может помочь избежать неожиданных проблем, связанных с ростом базы данных и производительностью. Дополнительную информацию о реорганизации базы данных смотрите в Техническое замечание 1683633.
- Чтобы уменьшить размер базы данных для серверов V7.1 и новее, введите следующие команды DB2 из каталога экземпляра сервера:

Ограничение: Команды могут увеличить число операций ввода-вывода и повлиять на производительность сервера. Чтобы свести к минимуму проблемы производительности, подождите выполнения одной команды перед вводом следующей команды. Команды DB2 можно вводить, когда сервер работает.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Чтобы увеличить или уменьшить размер активного журнала, выполните следующие шаги:
  1. Убедитесь, что в каталоге активного журнала достаточно пространства для увеличения размера журнала. Если существует зеркальная копия журнала, там, где она находится, также должно быть достаточно места для увеличения размера журнала.
  2. Отключите сервер.
  3. Измените в файле dsmserv.opt значение опции ACTIVELOGSIZE, задав новый размер активного журнала (в мегабайтах).
     Размер файла активного журнала основан на значении опции ACTIVELOGSIZE. Рекомендации по требованиям к объему пространства приведены в следующей таблице:

     Табл. 1. Как оценить требования к пространству томов и файлов

Значение опции ACTIVELOGSize	**Зарезервируйте этот объем свободного пространства в каталоге активного журнала в дополнение к пространству ACTIVELOGSize.**
16 ГБ - 128 ГБ	5120 МБ
129 ГБ - 256 ГБ	10240 МБ
257 ГБ - 512 ГБ	20480 МБ

     Чтобы изменить размер активного журнала до максимального размера, равного 512 ГБ, введите следующую серверную опцию:

     ```
     activelogsize 524288
     ```

  4. Если вы собираетесь использовать новый каталог активного журнала, измените имя каталога, заданное серверной опцией ACTIVELOGDIRECTORY. Новый каталог должен быть пустым, и он должен быть доступен для ID пользователя менеджера базы данных.
  5. Перезапустите сервер.
- Произведите сжатие архивных журналов, чтобы уменьшить объем пространства, необходимого для хранения. Разрешите динамическое сжатие архивного журнала следующей командой:

  ```
  setopt archlogcompress yes
  ```

  Ограничение: Будьте внимательны, если вы разрешаете опцию сервера ARCHLOGCOMPRESS на компьютерах с постоянным высоким использованием томов и высокими рабочими нагрузками. Разрешение этой опции в такой среде может привести к задержкам при архивировании файлов журнала из файловой системы активного журнала в файловую систему архивного журнала. Задержка может привести к тому, что в файловой системе активного журнала не хватит места. Обязательно выполняйте мониторинг пространства, доступного в файловой системе активного журнала, после разрешения сжатия архивного журнала. Если использование файловой системы каталога

активного журнала приближается к предельному, то запретите опцию сервера ARCHLOGCOMPRESS. Чтобы немедленно запретить сжатие архивного журнала без остановки сервера, введите команду SETOPT.

Ссылки, связанные с данной:
ACTIVELOGSIZE, серверная опция
EXTEND DBSPACE (увеличение емкости базы данных)
SETOPT (Задать динамическое обновление серверной опции)

Управление использованием памяти и процессора

Убедитесь, чтобы вы управляете требованиями к памяти и к использованию процессора, чтобы сервер мог выполнять такие процессы данных, как резервное копирование и дедупликация данных. Выполняя отдельные процессы, учитывайте их влияние на производительность.

Прежде чем начать

- Убедитесь, что в вашей конфигурации используются необходимые аппаратные и программные средства. Дополнительные сведения смотрите в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
- Дополнительную информацию об управлении ресурсами (например, база данных и журнал восстановления) смотрите в разделе Планирование массивов хранения.
- Добавьте больше системной памяти, чтобы определить, повышается ли при этом производительность. Регулярно отслеживайте использование памяти, чтобы определить, не требуется ли дополнительная память.

Процедура

1. Высвобождайте память из кэша файловой системы, если это возможно.
2. Для управления системной памятью, используемой каждым сервером в системе, используйте опцию DBMEMPERCENT. Ограничьте процентную долю системной памяти, которая может использоваться менеджером базы данных каждого сервера. Если все серверы равноценны, используйте для всех серверов одинаковые значения. Если один сервер является производственным сервером, а остальные серверы являются тест-серверами, задайте для производственного сервера более высокое значение, чем для тест-серверов.
3. Задайте для базы данных предельный объем данных пользователя и собственной памяти, чтобы не вырабатывать собственную память. Если собственная память будет исчерпана, это может приводить к ошибкам, снижению производительности ниже оптимальной и нестабильности.

Операционные системы Linux

Как узнать, поможет ли технология Aspera FASP оптимизировать передачу данных в вашей системной среде

Если ваш сервер IBM Spectrum Protect реплицирует узлы или защищает пулы хранения на удаленном сервере, определите, может ли технология Aspera Fast Adaptive Secure Protocol (FASP) повысить пропускную способность при передаче данных на удаленный сервер. Прежде чем включить технологию Aspera FASP, вы должны получить соответствующие лицензии. Доступна как лицензия на оценку, так и полная лицензия.

Прежде чем начать

Технология Aspera FASP используется для передачи экстентов данных из пула хранения контейнеров на удаленный сервер. Если технология Aspera FASP включена, экстенты данных при передаче всегда шифруются независимо от того, включен ли протокол Secure Sockets Layer (SSL). Однако если требуется защитить сетевое соединение, включите SSL. Информацию об SSL и о том, как включить SSL, смотрите в разделе Связь по протоколу Secure Sockets Layer и Transport Layer Security.

Об этой задаче

ограничения:

- Используйте технологию Aspera FASP, если в вашей региональной сети (wide area network, WAN) есть признаки высокой потери пакетов и/или задержки передачи данных, вызванных нарушениями в сети. Если

производительность WAN соответствует вашим бизнес-требованиям, не включайте технологию Aspera FASP.
- Чтобы включить технологию Aspera FASP для операций репликации узлов, данные должны храниться в пуле хранения каталога-контейнера.

Процедура

1. Определите, подходит ли технология Aspera FASP для вашей системной среды. Если не возникает ни одного из следующих условий, включите технологию Aspera FASP:
   - Средние задержки операций передачи данных превышают 50 мсек.
   - Потеря пакетов превышает 0,01%.

   Характеристики сетей могут сильно различаться. Возможно, вам удастся повысить пропускную способность сети, включив технологию Aspera FASP, даже если задержка при передаче данных составляет менее 40 мсек., а потеря пакетов - менее 0,01%.
2. Получите и установите соответствующие лицензии. Выполните одно из следующих действий.

   Получите и установите лицензии на оценку

   Чтобы получить и установить пробные лицензии сроком на 30 дней, выполните следующие действия:

   a. Затребуйте лицензии, отправив электронное письмо по адресу alliances@asperasoft.com:
      - Включите имя, адрес, номер телефона вашей компании, а также адрес электронной почты основного контактного лица вашей компании.
      - Укажите, что вам требуется 30-дневная лицензия на оценку.
      - Укажите нужное вам число лицензий.

      Для каждого сервера, используемого для передачи данных с использованием технологии Aspera FASP, требуется по одной лицензии. Например, если вы реплицируете узел с исходного сервера на сервер назначения, вам потребуется две лицензии.

      Если требование о выдаче лицензии будет утверждено, основное контактное лицо может ожидать поступления электронного письма в течение 24 часов. В электронное письмо будут вложены файлы лицензий, которым присваиваются имена в соответствии со следующими правилами:

      xxxxx-ConnectSrv-unlim.eval.aspera-license

      , где *xxxxx* – это уникальное число.

   b. Скопируйте один из файлов лицензии в каталог bin на исходном сервере. Выберите файл лицензии. Каталог по умолчанию:

      ```
      /opt/tivoli/tsm/server/bin
      ```

   c. Скопируйте остальные файлы лицензий в каталог bin на сервере назначения.
   d. На исходном сервере и на сервере назначения задайте для каждого файла лицензии уровень разрешений 755. Например, если вы используете каталог установки по умолчанию, а уникальный номер лицензии - 47474, введите одной строкой следующую команду:

      ```
      chmod 755 /opt/tivoli/tsm/server/bin/
      47474-ConnectSrv-unlim.eval.aspera-license
      ```

   Получите и установите полные лицензии.

   Чтобы получить и установить полные бессрочные лицензии, выполните следующие действия:

   a. Приобретите продукт IBM Spectrum Protect High Speed Data Transfer. Идентификационный номер продукта - 5725-Z10. Получить продукт можно на странице Passport Advantage.

      Для каждого сервера, используемого для передачи данных с использованием технологии Aspera FASP, требуется по одному экземпляру IBM Spectrum Protect High Speed Data Transfer. Например, если вы реплицируете узел с исходного сервера на сервер назначения, то вам потребуется два экземпляра IBM Spectrum Protect High Speed Data Transfer.

   b. Установите IBM Spectrum Protect High Speed Data Transfer на каждом сервере при помощи мастера установки.

   Ограничение: Если необходимые лицензии отсутствуют или истекли, операции по репликации узлов и защите пулов хранения с использованием технологии Aspera FASP завершатся неудачно.

3. Необязательно: Проверьте конфигурацию Aspera FASP, используя команду VALIDATE ASPERA. Команда VALIDATE ASPERA позволяет убедиться, что системная среда правильно сконфигурирована для Aspera FASP, а также проверить, установлены ли действительные лицензии. Кроме того, команду можно использовать, чтобы сравнить пропускную способность сети с технологией Aspera FASP и TCP/IP.

Дальнейшие действия

Чтобы включить технологию Aspera FASP, выполните шаги в разделе Оптимизация передачи данных путем включения технологии Aspera FASP.

- Оптимизация передачи данных путем включения технологии Aspera FASP
  Если вы используете удаленный сервер для защиты пула хранения или репликации узлов и столкнетесь с ошибками сети, разумным шагом с вашей стороны будет оптимизировать передачу данных, используя технологию Aspera Fast Adaptive Secure Protocol (FASP).

Планирование обновления сервера

Когда станет доступен пакет исправлений или промежуточное исправление, вы сможете обновить сервер IBM Spectrum Protect, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время. Перед обновлением сервера убедитесь, что вы выполнили шаги по планированию.

Об этой задаче

Выполните следующие рекомендации:

- Предпочтительный метод - обновить сервер с использованием мастера установки. Запустив мастер, щелкните в окне IBM Installation Manager по значку Обновить; не щелкайте по значкам Установить и Изменить.
- Если доступны обновления и для серверного компонента, и для компонента Центр операций, выберите переключатели, указывающие, что нужно обновить оба компонента.

Процедура

1. Проверьте список пакетов исправлений и промежуточных исправлений. Смотрите раздел Техническое замечание 1239415.
2. Ознакомьтесь с усовершенствованиями продукта, описанными в файлах readme.
   Совет: Получив пакет установки со страницы сайт поддержки IBM Spectrum Protect, вы также сможете получить доступ к файлу readme.
3. Убедитесь что версия, до которой вы обновляете сервер, совместима с другими компонентами, например, с агентами хранения и клиентами библиотек. Смотрите раздел Техническое замечание 1302789.
4. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены. Смотрите раздел Техническое замечание 1053218.
5. Прочтите инструкции по обновлению. Обязательно создайте резервную копию базы данных сервера, информации о конфигурации устройств и файла хронологии томов.

Дальнейшие действия

Чтобы установить пакет исправлений или промежуточное исправление, следуйте инструкциям для вашей операционной системы:

-  Операционные системы AIXУстановка пакета исправлений сервера IBM Spectrum Protect
- Операционные системы LinuxУстановка пакета исправлений сервера IBM Spectrum Protect
-  Операционные системы WindowsУстановка пакета исправлений сервера IBM Spectrum Protect

Тонкая настройка запланированных операций

Запланируйте ежедневное выполнение задач по обслуживанию, чтобы убедиться, что ваше решение работает правильно. Производя тонкую настройку решения, вы получаете максимальную отдачу от ресурсов сервера и эффективно используете другие функции, которые есть в вашем решении.

Процедура

1. Регулярно отслеживайте производительность системы, чтобы убедиться, что задачи по резервному копированию клиента и по обслуживанию сервера выполняются успешно. Следуйте инструкциям в Мониторинг решений по хранению.
2. Необязательно: Если информация мониторинга показывает, что рабочая нагрузка сервера повышается, смотрите информацию о планировании. Проверьте, является ли емкость системы достаточной, в следующих случаях:
   - Число клиентов увеличивается
   - Объем данных, резервное копирование которых производится, возрастает
   - Время, доступное для резервного копирования, изменяется
3. Определите, работает ли ваше решение на том уровне, который вы ожидаете. Проверьте расписания клиентов, чтобы выяснить, выполняются ли задачи в течение запланированного периода времени:
   a. Выберите клиента на странице Клиенты Центра операций.
   b. Щелкните по Сведения.
   c. На странице Сводка на клиенте проверьте операции Создана резервная копия и Реплицирован, чтобы выявить все риски.

   Скорректируйте время и частоту операций резервного копирования клиента, если потребуется.
4. Запланируйте достаточно времени для следующих задач по обслуживанию, чтобы они успешно выполнялись в течение 24-часового периода:
   a. Защищайте пулы хранения.
   b. Реплицируйте данные узлов.
   c. Создайте резервную копию базы данных.
   d. Запускайте обработку устаревания, чтобы удалить резервные и архивные копии файлов из серверного хранилища.

   Совет: Запланируйте задачи по обслуживанию, чтобы они запускались в соответствующее время в правильной последовательности. Например, запланируйте задачи репликации после успешного завершения операций по резервному копированию клиента.

- Перемещение клиентов с одного сервера на другой
  Чтобы не допустить нехватки пространства на сервере или устранить проблемы рабочей нагрузки, вам может потребоваться переместить клиентские узлы с одного сервера на другой.

Понятия, связанные с данным:
Производительность
Задачи, связанные с данной:
Дедупликация данных (V7.1.1)

Управление операциями клиентов

Вы можете оценить и устранить ошибки, связанные с клиентом резервного копирования и архивирования, используя компонент Центр операций, который предоставляет рекомендации по устранению ошибок. В случае ошибок на клиентах других типов вам следует изучить журналы ошибок на клиенте и ознакомиться с документацией по продукту.

Об этой задаче

В некоторых случаях ошибки клиентов можно устранить, остановив и перезапустив приемник клиента. Если клиентские узлы или ID администратора окажутся заблокированы, вы сможете устранить проблему, разблокировав клиентский узел или ID администратора, а затем переустановив пароль.

Подробные инструкции по выявлению и устранению ошибок клиентов смотрите в разделе Устранение проблем клиентов.

- Изменение объема резервного копирования клиента
  При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.
- Оценка ошибок в журналах ошибок клиентов
  Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.
- Остановка и перезапуск приемника клиента
  Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

- Изменение паролей
  Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.
- Списание клиентского узла
  Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).
- Деактивация данных для высвобождения пространства хранения
  В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.
- Управление обновлениями клиентов
  Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Изменение объема резервного копирования клиента

При настройке операций резервного копирования клиента предпочтительной практикой является исключение объектов, которые вам не требуются. Например, обычно имеет смысл исключить из операции резервного копирования временные файлы.

Об этой задаче

Исключение ненужных объектов из операций резервного копирования позволяет лучше контролировать объем пространства хранения, необходимого для операций резервного копирования, а также расходы на хранение. В зависимости от вашего пакета лицензирования вам, возможно, также удастся ограничить расходы, связанные с лицензированием.

Процедура

То, как вы изменяете масштаб операций по резервному копированию, зависит от продукта, установленного на клиентском узле:

- Для клиента резервного копирования и архивирования можно создать список включения-исключения, чтобы включить файлы, группы файлов или каталоги в операции резервного копирования или исключить их из этих операций. Чтобы создать список включения-исключения, следуйте инструкциям в разделе Создание списка include-exclude.

  Чтобы обеспечить непротиворечивое использование списка включения-исключения для всех клиентов одного типа, можно создать на сервере набор опций клиента, содержащий необходимые опции. Затем вы назначаете набор опций клиента каждому из клиентов того же типа. Дополнительные сведения смотрите в разделе Управление операциями клиента через наборы опций клиентов.

- Для клиента резервного копирования и архивирования можно задать объекты в операции инкрементного резервного копирования, используя опцию domain. Следуйте инструкциям в разделе Domain, опция.
- В случае других продуктов, чтобы указать, какие объекты включаются в операции резервного копирования, а какие - исключаются из этих операций, следуйте инструкциям в документации по продукту.

Оценка ошибок в журналах ошибок клиентов

Ошибки клиента можно устранить, получив рекомендации из компонента Центр операций или просмотрев журналы ошибок на клиенте.

Прежде чем начать

Чтобы устранить ошибки на клиенте резервного копирования и архивирования в операционной системе Linux или Windows, убедитесь, что у вас установлена и запущена служба служба управления клиентами. Инструкции по установке

смотрите в разделе Сбор диагностической информации с использованием служб управления клиентом.

Процедура

Чтобы диагностировать и устранить ошибки клиента, выполните одно из следующих действий:

- Если служба служба управления клиентами установлена на клиентском узле, выполните следующие шаги:
  1. На странице обзора в компоненте Центр операций щелкните по Клиенты и выберите клиент.
  2. Щелкните по Сведения.
  3. На странице Сводка клиента щелкните по вкладке Диагностика.
  4. Прочтите полученные сообщения журнала.
     Советы:
     - Чтобы показать или скрыть панель Журналы клиента, дважды щелкните по строке Журналы клиента.
     - Чтобы изменить размер панели Журналы клиента, щелкните по строке Журналы клиента и перетащите ее в нужное положение.

     Если на странице Диагностика показаны рекомендации, выберите рекомендацию. В панели Журналы клиента сообщения журнала клиента, с которыми связаны рекомендации, выделены.
  5. Используйте рекомендации, чтобы устранить проблемы, указанные в сообщениях об ошибках.
     Совет: Рекомендации предоставляются не для всех сообщений клиентов.
- Если служба служба управления клиентами не установлена на клиентском узле, смотрите журналы ошибок установленного клиента.

Остановка и перезапуск приемника клиента

Если вы измените конфигурацию вашего решения, вам нужно будет перезапустить приемник клиента на всех клиентских узлах, где установлен клиент резервного копирования и архивирования.

Об этой задаче

В некоторых случаях ошибки планирования клиентов можно устранить, остановив и перезапустив приемник клиента. Чтобы запланированные операции могли выполняться на клиенте, приемник клиента должен работать. Например, если вы измените IP-адрес или имя домене сервера, вы должны будете перезапустить приемник клиента.

Процедура

Следуйте инструкциям для операционной системы, установленной на клиентском узле:

AIX и Oracle Solaris

- Чтобы остановить приемник клиента, выполните следующие действия:
  a. Определите ID процесса приемника клиента, введя в командной строке следующую команду:

     ```
     ps -ef | grep dsmcad
     ```

     Ознакомьтесь с выводом. В приведенном ниже примере выходной информации 6764 - это ID процесса приемника клиента:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Введите следующую команду в командной строке:

     ```
     kill -9 PID
     ```

     где *PID* задает ID процесса приемника клиента.
- Чтобы запустить приемник клиента, введите в командной строке следующую команду:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Чтобы остановить приемник клиента (но не перезапускать его), введите следующую команду:

  ```
  # service dsmcad stop
  ```

- Чтобы остановить и перезапустить приемник клиента, введите следующие команды:

  ```
  # service dsmcad restart
  ```

MAC OS X

Выберите Приложения > Утилиты > Терминал.

- Чтобы остановить приемник клиента, введите следующую команду:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```

- Чтобы запустить приемник клиента, введите следующую команду:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Чтобы остановить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Остановить и OK.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
  a. Выберите Пуск > Администрирование > Службы.
  b. Дважды щелкните по службе приемника клиента.
  c. Щелкните по Запуск и OK.

Ссылки, связанные с данной:
Устранение проблем расписаний клиентов

Изменение паролей

Если пароль для клиентского узла или ID администратора окажется потерян или забыт, вы можете переустановить пароль. Если будет предпринято несколько попыток получить доступ к системе с использованием неправильного пароля, это может привести к блокировке клиентского узла или ID администратора. Вы можете выполнить ряд шагов, чтобы устранить эту проблему.

Процедура

Чтобы устранить ошибки паролей, выполните одно из следующих действий:

- Если клиент резервного копирования и архивирования установлен на клиентском узле, а пароль был потерян или забыт, выполните следующие шаги:
  1. Сгенерируйте новый пароль, введя команду UPDATE NODE:

     ```
     update node имя_узла
     новый_пароль forcepwreset=yes
     ```

     где *имя_узла* - это клиентский узел, а *новый_пароль* - это пароль, который вы назначаете.
  2. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
     Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.
- Если администратор окажется заблокирован из-за проблем, связанных с паролем, выполните следующие шаги:
  1. Чтобы обеспечить администратору доступ к серверу, введите команду UNLOCK ADMIN. Инструкции смотрите в разделе UNLOCK ADMIN (разблокирование администратора).
  2. Задайте новый пароль, используя команду UPDATE ADMIN:

     ```
     update admin имя_администратора
     новый_пароль
     forcepwreset=yes
     ```

     где *имя_администратора* - это имя администратора, а *новый_пароль* - это пароль, который вы назначаете.
- Если клиентский узел заблокирован, выполните следующие шаги:

1. Определите, почему клиентский узел заблокирован и нужно ли его разблокировать. Например, если клиентский узел окажется списан, он удаляется из производственной среды. Обратить операцию списания нельзя, и клиентский узел останется заблокированным. Клиентский узел также может оказаться заблокированным, если данные клиента являются предметом юридического изучения.
2. Если вам нужно разблокировать клиентский узел, используйте команду UNLOCK NODE. Инструкции смотрите в разделе UNLOCK NODE (Разблокировать клиентский узел).
3. Сгенерируйте новый пароль, введя команду UPDATE NODE:

   ```
   update node имя_узла
   новый_пароль forcepwreset=yes
   ```

   где *имя_узла* задает имя узла, а *новый_пароль* - это пароль, который вы назначаете.
4. Проинформируйте владельца клиентского узла об измененном пароле. Когда владелец клиентского узла входит в систему с использованием указанного пароля, новый пароль генерируется автоматически. Этот пароль неизвестен пользователям, чтоб позволяет сделать защиту более строгой.
   Совет: Пароль генерируется автоматически, если вы ранее задали для опции passwordaccess значение `generate` в файле опций клиента.

Списание клиентского узла

Если клиентский узел больше не требуется, можно запустить процесс для его удаления из производственной среды. Например, если рабочая станция производила резервное копирование данных на сервер IBM Spectrum Protect, но рабочая станция больше не используется, рабочую станцию можно списать (вывести из использования).

Об этой задаче

При запуске процесса списания сервер блокирует клиентский узел, чтобы помешать ему получить доступ к серверу. Файлы, принадлежащие клиентскому узлу, постепенно удаляются, и затем удаляется клиентский узел. Можно списать следующие типы клиентских узлов:

Клиентские узлы приложения
: К клиентским узлам приложений относятся серверы электронной почты, базы данных и другие приложения. Например, клиентским узлом приложения может быть любое из следующих приложений:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Клиентские узлы компьютеров
: В число клиентских узлов компьютеров входят рабочие станции, серверы файлов NAS и клиенты API.

Клиентские узлы виртуальных машин
: Клиентские узлы виртуальных машин представляют собой отдельные хосты-гости в гипервизоре. Каждая виртуальная машина представлена как файловое пространство.

Простейший метод списания клиентского узла заключается в том, чтобы использовать Центр операций. Процесс списания выполняется в фоновом режиме. Если клиент сконфигурирован для репликации данных клиента, Центр операций, прежде чем списать клиент, автоматически удалит клиент из репликации на исходном и целевом серверах репликации.
Совет: Либо можно списать клиентский узел, введя команду DECOMMISSION NODE или DECOMMISSION VM. Вы можете счесть целесообразным использовать этот метод в следующих случаях:

- Чтобы запланировать процесс списания на будущее или выполнить ряд команд, используя сценарий, задайте выполнение процесса списания в фоновом режиме.
- Чтобы производить мониторинг процесса списания с целью отладки, задайте выполнение процесса списания в фоновом режиме. Если вы запустите процесс в активном режиме, вам придется дождаться завершения процесса, прежде чем вы сможете перейти к другим задачам.

Процедура

Выполните одно из следующих действий.

- Чтобы списать клиент в фоновом режиме, используя Центр операций, выполните следующие действия:

1. На странице Обзор для компонента Центр операций щелкните по Клиенты и выберите клиент.
2. Выберите Еще > Списать.

- Чтобы списать клиентский узел, используя команду администрирования, выполните следующие действия:
  1. Определите, сконфигурирован ли клиентский узел для репликации узла, введя команду QUERY NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

     ```
     query node austin format=detailed
     ```

     Проверьте выходное поле Состояние репликации.
  2. Если клиентский узел сконфигурирован для репликации, удалите клиентский узел из репликации, введя команду REMOVE REPLNODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

     ```
     remove replnode austin
     ```

  3. Выполните одно из следующих действий.
     - Чтобы списать клиентские узлы приложений или системные клиентские узлы в фоновом режиме, введите команду DECOMMISSION NODE. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

       ```
       decommission node austin
       ```

     - Чтобы списать клиентские узлы приложений или системные клиентские узлы в активном режиме, введите команду DECOMMISSION NODE и задайте параметр `wait=yes`. Например, если имя клиентского узла - AUSTIN, введите следующую команду:

       ```
       decommission node austin wait=yes
       ```

     - Чтобы списать виртуальную машину в фоновом режиме, введите команду DECOMMISSION VM. Например, если имя виртуальной машины - AUSTIN, файловое пространство - 7, а имя файлового пространства задано с помощью ID файлового пространства, введите следующую команду:

       ```
       decommission vm austin 7 nametype=fsid
       ```

       Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

       ```
       decommission vm "austin 2" 7 nametype=fsid
       ```

     - Чтобы списать виртуальную машину в активном режиме, введите команду DECOMMISSION VM и задайте параметр `wait=yes`. Например, введите следующую команду:

       ```
       decommission vm austin 7 nametype=fsid wait=yes
       ```

       Если имя виртуальной машины содержит один или несколько пробелов, заключите имя в двойные кавычки. Например:

       ```
       decommission vm "austin 2" 7 nametype=fsid wait=yes
       ```

Дальнейшие действия

Следите за сообщениями об ошибках, которые могут появиться в пользовательском интерфейсе или в выходной информации команды сразу после запуска процесса.

Можно проверить, списан ли клиентский узел:

1. Щелкните на странице Обзор в компоненте Центр операций по Клиенты.
2. В таблице Клиенты проверьте состояние в столбце Под угрозой:
   - Состояние DECOMMISSIONED (Списан) указывает, что узел списан.
   - Нулевое значение указывает, что узел не списан.
   - Состояние PENDING (Отложено) указывает, что узел списывается или процесс списания завершился неудачно.

   Совет: Если вы хотите определить состояние отложенного процесса списания, введите следующую команду:

   ```
   query process
   ```

3. Ознакомьтесь с выводом команды:
   - Если указано состояние для процесса списания, процесс выполняется. Например:

```
query process

 Номер       Описание процесса                  Состояние процесса
  Число
--------     --------------------     -----------------------------------------
       3          DECOMMISSION NODE        Number of backup objects deactivated
                                           for node NODE1: 8 objects deactivated.
```

- Если для процесса списания никакого состояния не указано и вы не получили сообщения об ошибке, процесс не завершен. Процесс может быть не завершен, если файлы, связанные с узлом, еще не деактивированы. После деактивации файлов снова запустите процесс списания.
- Если для процесса списания никакого состояния не указано и вы получили сообщения об ошибке, это означает, что процесс завершился неудачно. Еще раз запустите процесс списания.

Ссылки, связанные с данной:
DECOMMISSION NODE (Списать клиентский узел)
DECOMMISSION VM (Списать виртуальную машину)
QUERY NODE (Запросить информацию об узлах)
REMOVE REPLNODE (Удалить клиентский узел из репликации)

Деактивация данных для высвобождения пространства хранения

В некоторых случаях можно деактивировать данные, хранящиеся на сервере IBM Spectrum Protect. Когда вы запустите процесс деактивации, все резервные копии данных, сохраненные до указанной даты и времени, деактивируются и будут удалены, когда истечет срок их действия. Таким способом можно высвободить пространство на сервере.

Об этой задаче

Некоторые клиенты приложений всегда сохраняют данные на сервере как активные резервные копии данных. Поскольку активные резервные копии данных не управляются политиками устаревания перечня, данные не удаляются автоматически, и серверное хранилище используется до бесконечности. Чтобы высвободить пространство хранения, используемое устаревшими данными, можно деактивировать данные.

Когда вы запускаете процесс деактивации, все активные резервные копии данных, сохраненные до указанной даты, станут неактивными. Данные будут удалены по мере истечения срока их хранения, и восстановить их будет нельзя. Функция деактивации применяется только к клиентам приложений, которые защищают базы данных Oracle.

Процедура

1. На странице обзора в компоненте Центр операций щелкните по Клиенты.
2. В таблице Клиенты выберите один или несколько клиентов и щелкните по Еще > Очистить.
   Метод командной строки: Деактивируйте данные, используя команду DEACTIVATE DATA.

Ссылки, связанные с данной:
DEACTIVATE DATA (деактивация данных для клиентского узла)

Управление обновлениями клиентов

Когда появится пакет исправлений или промежуточное исправление для клиента, вы сможете обновить клиент, чтобы воспользоваться преимуществами в улучшенном продукте. Серверы и клиенты можно обновлять в разное время, и они могут находиться на разных уровнях (с некоторыми ограничениями).

Прежде чем начать

1. Прочтите требования к совместимости клиентов/серверов в разделе Техническое замечание 1053218. Если ваше решение включает в себя серверы или клиенты с более ранним уровнем версии, чем V7.1, смотрите рекомендации, чтобы убедиться, что операции резервного копирования и архивирования клиента не будут нарушены.
2. Узнайте о требованиях к системе для клиента в разделе Поддерживаемые операционные системы для IBM Spectrum Protect.
3. Если решение содержит агенты хранения или библиотечные клиенты, ознакомьтесь с информацией о совместимости агентов хранения и библиотечных клиентов с серверами, сконфигурированными в качестве менеджеров библиотек. Смотрите раздел Техническое замечание 1302789.

Если вы собираетесь обновить менеджера библиотек и библиотечный клиент, сначала нужно обновить менеджера библиотек.

Процедура

Для обновления программного обеспечения выполните инструкции, перечисленные в следующей таблице.

Программа	Ссылка на инструкции
Клиент резервного копирования и архивирования IBM Spectrum Protect	• Планирование обновлений клиента
IBM Spectrum Protect Snapshot	• Установка и обновление IBM Spectrum Protect Snapshot для UNIX и Linux • Установка и обновление IBM Spectrum Protect Snapshot для VMware • Установка и обновление IBM Spectrum Protect Snapshot для Windows
IBM Spectrum Protect for Databases	• Обновление Data Protection for SQL Server • Установка Data Protection for Oracle • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Обновление IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Установка Data Protection for IBM Domino в системе UNIX, AIX или Linux (V7.1.0) • Установка Data Protection for IBM Domino в системе Windows (V7.1.0) • Установка, обновление и перенастройка IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Установка и обновление Data Protection for VMware • Установка Data Protection for Microsoft Hyper-V

Управление Центром операций

Центр операций предоставляет веб-доступ и мобильный доступ к информации о состоянии для среды IBM Spectrum Protect. Используйте Центр операций для мониторинга нескольких серверов и для выполнения некоторых задач администрирования. Кроме того, Центр операций предоставляет веб-клиент для командной строки IBM Spectrum Protect.

- Добавление и удаление подчиненных серверов
  В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.
- Запуск и остановка веб-сервера
  Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.
- Перезапуск мастера начального конфигурирования
  Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.
- Изменение хаб-сервера
  Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.
- Восстановление конфигурации до предварительно сконфигурированного состояния
  При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до

предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Добавление и удаление подчиненных серверов

В среде с несколькими серверами можно подключить к хаб-серверу дополнительные серверы, которые называются *подчиненные серверы*.

Об этой задаче

Подчиненные серверы отправляют оповещения и информацию о состоянии хаб-серверу. Центр операций содержит консолидированное представление оповещений и информации о состоянии для хаб-сервера и всех подчиненных серверов.

- Добавление подчиненного сервера
  После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.
- Удаление подчиненного сервера
  Можно удалить подчиненный сервер из Центра операций.

Добавление подчиненного сервера

После конфигурирования хаб-сервера для Центр операций можно добавить к этому хаб-серверу один или несколько подчиненных серверов.

Прежде чем начать

Связь между подчиненным сервером и хаб-сервером должна быть защищена с использованием протокола Transport Layer Security (TLS). Для защиты связи добавьте сертификат подчиненного сервера в файл доверенных сертификатов хаб-сервера.

Процедура

1. Щелкните в панели меню Центр операций по Серверы. Откроется страница Серверы.

   В таблице на странице Серверы состоянием сервера может быть "Не отслеживается" Это состояние означает, что хотя администратор и определил этот сервер на хаб-сервере при помощи команды DEFINE SERVER, этот сервер еще не сконфигурирован в качестве подчиненного сервера.

2. Выполните одно из следующих действий:
   - Щелкните по серверу, чтобы выделить его, и щелкните в панели меню таблицы по Отслеживать подчиненный.
   - Если сервера, который вы хотите добавить, нет в таблице, а защищенная связь SSL/TLS не требуется, то щелкните по + Подчиненный в панели меню таблицы.
3. Задайте нужную информацию и выполните действия в мастере конфигурирования подчиненных серверов.
   Совет: Если срок хранения записи события сервера меньше 14 дней, то для него автоматически задается значение 14 дней, если сервер конфигурируется как подчиненный сервер.

Удаление подчиненного сервера

Можно удалить подчиненный сервер из Центра операций.

Об этой задаче

Вам может потребоваться удалить подчиненный сервер, например, в следующих ситуациях:

- Вы хотите переместить подчиненный сервер с одного хаб-сервера на другой.
- Подчиненный сервер больше не нужен.

Процедура

Чтобы удалить подчиненный сервер из группы серверов, которая управляется хаб-сервером, сделайте следующее:

1. В командной строке IBM Spectrum Protect введите следующую команду для хаб-сервера:

   ```
   QUERY MONITORSETTINGS
   ```

2. Скопируйте в выходных результатах команды имя, указанное в поле Отслеживаемые группы.
3. Введите на хаб-сервере следующую команду, где *имя_группы* - это имя отслеживаемой группы, а *имя_члена* - это имя подчиненного сервера.

   ```
   DELETE GRPMEMBER имя_группы имя_члена
   ```

4. Необязательно: Если вы хотите переместить подчиненный сервер с одного хаб-сервера на другой, **не** выполняйте этот шаг. В ином случае можно запретить оповещения и мониторинг для подчиненного сервера, введя на подчиненном сервере следующие команды:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Необязательно: Если определение подчиненного сервера используется в других целях, например, для конфигурирования предприятия, маршрутизации команд, хранения виртуальных томов или управления библиотекой, **не** выполняйте этот шаг. В противном случае можно удалить определение подчиненного сервера на хаб-сервере, введя на хаб-сервере следующую команду:

   ```
   DELETE SERVER имя_подчиненного_сервера
   ```

   Совет: Если определение сервера удаляется сразу же после удаления сервера из отслеживаемой группы, информация о состоянии сервера может остаться в центре операций на неопределенно долгое время.

   Чтобы избежать этой проблемы, перед удалением определения сервера дождитесь, когда пройдет интервал сбора состояния. Интервал сбора данных состояния показан на странице Параметры в центре операций.

Запуск и остановка веб-сервера

Веб-сервер Центра операций работает как служба и запускается автоматически. Вам может потребоваться остановить и повторно запустить Web-сервер, например, чтобы произвести изменения конфигурации.

Процедура

1. Остановите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./stopserver.sh
     ```

   - Операционные системы LinuxВведите следующую команду:

     ```
     service opscenter.rc stop
     ```

   - Операционные системы WindowsВ окне Службы остановите службу Центр операций IBM Spectrum Protect.
2. Запустите веб-сервер.
   - Операционные системы AIXВ каталоге /*каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:

     ```
     ./startserver.sh
     ```

   - Операционные системы LinuxВведите следующие команды:

     Запустите сервер:

     ```
     service opscenter.rc start
     ```

     Перезапустите сервер:

     ```
     service opscenter.rc restart
     ```

     Определите, работает ли сервер:

```
service opscenter.rc status
```

- Операционные системы WindowsВ окне Службы запустите службу Центр операций IBM Spectrum Protect.

Перезапуск мастера начального конфигурирования

Вам может потребоваться повторно запустить мастер по начальному конфигурированию Центр операций, например, для внесения изменений в конфигурацию.

Прежде чем начать

Чтобы изменить следующие параметры, используйте страницу Параметры в Центр операций вместо перезапуска мастера начального конфигурирования:

- Периодичность обновления данных
- Интервал времени, в течение которого предупреждение активно, неактивно или закрывается
- Условия, обозначающие риск для клиентов

Центр операций помогает включить дополнительную информацию о том, как изменить эти параметры.

Об этой задаче

Для перезапуска мастера начального конфигурирования необходимо удалить файл свойств с информацией о соединении с хаб-сервером. Однако никакие настройки оповещений, мониторинга, состояния 'Под угрозой' или среды для нескольких серверов, заданные для хаб-сервера, не удаляются. Эти настройки используются как настройки мастера конфигурирования по умолчанию при его перезапуске.

Процедура

1. Остановите веб-сервер Центр операций.
2. На компьютере с установленным продуктом Центр операций перейдите в следующий каталог, где *каталог_установки* представляет собой каталог, в котором установлен продукт Центр операций:
   - Операционные системы AIXОперационные системы Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windows*каталог_установки*\ui\Liberty\usr\servers\guiServer

   Например:
   - Операционные системы AIXОперационные системы Linux/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Операционные системы Windowsc:\Program Files\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Удалите из каталога guiServer файл serverConnection.properties.
4. Запустите веб-сервер Центра операций.
5. Откройте Центр операций.
6. Переконфигурируйте Центр операций при помощи мастера конфигурирования. Задайте новый пароль для ID администратора мониторинга.
7. На каждом из подчиненных серверов, ранее связанных с хаб-сервером, измените пароль для ID администратора мониторинга, введя следующую команду в интерфейсе командной строки IBM Spectrum Protect:

   ```
   UPDATE ADMIN  IBM-OC-имя_хаб-сервера новый_пароль
   ```

   Ограничение: Не изменяйте никакие другие параметры для этого ID администратора. После того, как задан начальный пароль, он автоматически управляется Центр операций.

Изменение хаб-сервера

Можно использовать Центр операций удалить хаб-сервер IBM Spectrum Protect и сконфигурированm другой хаб-сервер.

Процедура

1. Перезапустите мастер начального конфигурирования Центр операций. При выполнении этой процедуры вы удаляете соединение хаб-сервера.
2. При помощи мастера сконфигурируйте Центр операций для соединения с новым хаб-сервером.

Задачи, связанные с данной:

Восстановление конфигурации до предварительно сконфигурированного состояния

При возникновении некоторых проблем может понадобиться восстановление конфигурации Центр операций до предварительно сконфигурированного состояния, когда серверы IBM Spectrum Protect не определены как хаб-серверы или подчиненные серверы.

Процедура

Чтобы восстановить конфигурацию, выполните следующие шаги:

1. Остановите веб-сервер Центр операций.
2. Деконфигурируйте хаб-сервер, выполнив следующие действия:
   a. Введите на хаб-сервере следующие команды:

   ```
   SET MONITORINGADMIN ""
   SET MONITOREDSERVERGROUP ""
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   REMOVE ADMIN IBM-OC-имя_хаб-сервера
   ```

   Совет: `IBM-OC-`*`имя_хаб-сервера`* - это ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Переустановите пароль для хаб-сервера, введя на хаб-сервере следующую команду:

   ```
   SET SERVERPASSWORD ""
   ```

   Внимание: Не выполняйте этот шаг, если хаб-сервер сконфигурирован с другими серверами для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.
3. Отмените конфигурацию всех подчиненных серверов, выполнив следующие шаги:
   a. Чтобы определить, остаются ли какие-либо подчиненные серверы как члены группы серверов, введите на хаб-сервере следующую команду:

   ```
   QUERY SERVERGROUP IBM-OC-имя_хаб-сервера
   ```

   Совет: `IBM-OC-`*`имя_хаб-сервера`* - это имя отслеживаемой группы серверов, которая была автоматически создана при конфигурировании первого подчиненного сервера. Это имя группы серверов - это также ID администратора мониторинга, который был автоматически создан при начальном конфигурировании хаб-сервера.
   b. Чтобы удалить из группы серверов подчиненные серверы, введите на хаб-сервере следующую команду для каждого подчиненного сервера:

   ```
   DELETE GRPMEMBER IBM-OC-имя_хаб-сервера имя_подчиненного_сервера
   ```

   c. После удаления всех подчиненных серверов из группы серверов введите следующую команду на хаб-сервере:

   ```
   DELETE SERVERGROUP IBM-OC-имя_хаб-сервера
   SET MONITOREDSERVERGROUP ""
   ```

   d. Введите на каждом подчиненном сервере следующую команду:

   ```
   REMOVE ADMIN IBM-OC-имя_хаб-сервера
   SETOPT PUSHSTATUS NO
   SET ALERTMONITOR OFF
   SET STATUSMONITOR OFF
   ```

   e. Удалите на каждом из подчиненных серверов определение хаб-сервера, введя на серверах следующую команду:

   ```
   DELETE SERVER имя_хаб_сервера
   ```

   Внимание: Не выполняйте этот шаг, если данное определение используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.

f. Удалите на хаб-сервере определение каждого из подчиненных серверов, введя следующую команду:

```
DELETE SERVER имя_подчиненного_сервера
```

Внимание: Не выполняйте этот шаг, если данное определение сервера используется для других целей, таких как совместное использование библиотек, экспорт и импорт данных или репликация узлов.

4. Восстановите параметры по умолчанию для каждого сервера, введя следующие команды:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Перезапустите мастер начального конфигурирования Центр операций.

Задачи, связанные с данной:
Перезапуск мастера начального конфигурирования
Запуск и остановка веб-сервера

Конфигурирование виртуальных ленточных библиотек

Виртуальная ленточная библиотека (Virtual Tape Library, VTL) не использует физические ленточные носители. При реализации хранилища VTL вы не ограничены емкостью физической ленточной библиотеки. Возможность определения многих томов и накопителей может обеспечить большую гибкость для среды хранения.

- Особенности использования виртуальных ленточных библиотек
  Есть некоторые особенности при определении библиотеки в качестве виртуальной ленточной библиотеки (VTL), касающиеся повышения производительности и конфигурации оборудования.
- Добавление виртуальной ленточной библиотеки в вашу среду
  Определите виртуальную лентночную библиотеку (virtual tape library, VTL), чтобы воспользоваться преимуществами производительности и лучшей масштабируемости.
- Определение всех накопителей и путей для одной библиотеки
  Команда PERFORM LIBACTION служит для конфигурирования одной библиотеки SCSI или виртуальной ленточной библиотеки (VTL) за один шаг.
- Операционные системы AIXОперационные системы LinuxПример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей
  Конфигурирование библиотеки VTL или SCSI, содержащей два ленточных накопителя LTO.
- Операционные системы AIXОперационные системы LinuxПример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей
  Вы можете сконфигурировать библиотеку с накопителями нескольких типов, например, библиотеку StorageTek L40, содержащую один накопитель DLT и один накопитель LTO Ultrium.

Особенности использования виртуальных ленточных библиотек

Есть некоторые особенности при определении библиотеки в качестве виртуальной ленточной библиотеки (VTL), касающиеся повышения производительности и конфигурации оборудования.

Об этой задаче

Определение VTL на сервере IBM Spectrum Protect может помочь повысить производительность, так как сервер выполняет обработку точек монтирования для библиотек VTL иначе, чем для реальных ленточных библиотек. Физические ограничения реальных ленточных устройств не действуют для VTL, что создает лучшие возможности для масштабирования.

Любую виртуальную ленточную библиотеку можно определить как VTL, когда выполняются следующие условия:

- В VTL не используются неоднородные носители. В библиотеке эмулируется только один тип и поколение дисков и носителей.
- У каждого сервера и агента хранения с доступом к VTL есть пути, заданные для всех накопителей в библиотеке.

Если какие-либо из этих условий не выполняются, все преимущества в производительности монтирования от определения библиотеки как VTL на сервере IBM Spectrum Protect сокращаются или исчезают.

Библиотеки VTL совместимы с блоее ранними версиями как библиотечных клиентов, так и агентов хранения. На библиотечный клиент или на агент хранения не влияет тип библиотеки, используемый для хранения. Если для библиотеки SCSI выполняются условия на неоднородные носители и пути, ее можно определить или переопределить, как LIBTYPE=VTL.

- Емкость хранения для виртуальных ленточных библиотек
  Поскольку у виртуальных ленточных библиотек (virtual tape libraries, VTL) нет физических ограничений, как у реальных ленточных устройств, они отличаются более гибкой емкостью хранения.
- Конфигурация накопителей для виртуальных ленточных библиотек
  Конфигурация накопителей для виртуальных ленточных библиотек (virtual tape library, VTL) зависит от потребностей вашей среды.

Емкость хранения для виртуальных ленточных библиотек

Поскольку у виртуальных ленточных библиотек (virtual tape libraries, VTL) нет физических ограничений, как у реальных ленточных устройств, они отличаются более гибкой емкостью хранения.

Понятие емкости виртуальной ленточной библиотеки отличается от емкости физического ленточного устройства. В физической ленточной библиотеке у каждого тома есть определенная емкость, и емкость всей библиотеки определяется общим числом ее томов. В отличие от этого, емкость VTL определяется объемом доступного дискового пространства. Количество томов на диске и их объем можно увеличивать и уменьшать.

От этих параметров зависит, что понимается под исчерпанием места на диске в VTL. Например, в одном из томов VTL свободное пространство может закончиться до достижения назначенной этому тому емкости, если не останется места на базовом диске в целом. В этой ситуации сервер может получить сообщение о конце тома без предупреждений, что может привести к ошибкам резервного копирования.

В случае возникновения ошибок нехватки памяти и резервного копирования дисковое пространство обычно по-прежнему доступно в VTL. Оно скрыто в неиспользуемых томах. Например, тома, которые были логически удалены или возвращены в чистое состояние на сервере IBM Spectrum Protect, удаляются только из базы данных сервера. VTL не получает никакого уведомления и поддерживает полный объем тома, выделенный в соответствии с замечаниями по его емкости.

Чтобы помочь предотвратить ошибки нехватки памяти, убедитесь, что при обновлении всех библиотек SCSI до LIBTYPE=VTL для параметра RELABELSCRATCH задано значение YES. Опция RELABELSCRATCH позволяет серверу перезаписывать метку для любого тома, который был удален, и возвращать этот том в библиотеке в чистое состояние. По умолчанию для параметра RELABELSCRATCH для всех библиотек, определенных как VTL, используется значение YES.

Ссылки, связанные с данной:
UPDATE LIBRARY (обновление библиотеки)

Конфигурация накопителей для виртуальных ленточных библиотек

Конфигурация накопителей для виртуальных ленточных библиотек (virtual tape library, VTL) зависит от потребностей вашей среды.

В большинстве сред VTL используется как можно больше накопителей, чтобы максимизировать число параллельных операций с лентами. Монтирование ленты в среде VTL обычно выполняется быстрее, чем монтирование физической ленты. Однако слишком большое число используемых накопителей ведет к увеличению времени, затрачиваемого сервером IBM Spectrum Protect в ответ на требование монтирования. Процесс выбора отнимает больше времени, поскольку число накопителей, определенных в одном объекте библиотеки на сервере, возрастает. Монтирование виртуальной ленты может занять столько же или больше времени, чем монтирование физической ленты, в зависимости от числа накопителей в VTL.

Для наилучших результатов при создании накопителей уточните у поставщика VTL рекомендации по поводу конкретных устройств. Если для каждого VTL требуется больше 300-500 накопителей, можно ввести логическое разделение VTL на несколько библиотек и назначить накопители каждой библиотеке. Операционная система и аппаратные конфигурации SAN могут накладывать ограничения на число устройств, которые могут использоваться в библиотеке VTL.

Добавление виртуальной ленточной библиотеки в вашу среду

Определите виртуальную ленточную библиотеку (virtual tape library, VTL), чтобы воспользоваться преимуществами производительности и лучшей масштабируемости.

Об этой задаче

VTL определяются при помощи команды DEFINE LIBRARY с параметром LIBTYPE=VTL. Поскольку функционально библиотека VTL взаимодействует с сервером точно так же, как библиотека SCSI, можно использовать команду UPDATE LIBRARY для изменения типу уже определенной библиотеки SCSI. Нет необходимости переопределять эту библиотеку.

Процедура

- Добавьте новую библиотеку VTL. Задайте библиотеку как VTL для сервера, как показано в следующем примере:

  ```
  define library chester libtype=vtl
  ```

  Это конфигурирует новую библиотеку VTL и включает опцию RELABELSCRATCH для перемаркировки томов, которые удаляются и возвращаются в состояние чистых.

- Обновите библиотеку SCSI для VTL. Если у вас есть библиотека SCSI, и вы хотите использовать ее как VTL, измените тип этой библиотеки при помощи команды UPDATE LIBRARY:

  ```
  update library calzone libtype=vtl
  ```

  Эту команду можно ввести, только если обновляемая библиотека задана с использованием параметра LIBTYPE=SCSI.

Ссылки, связанные с данной:
DEFINE LIBRARY (Задать библиотеку)
UPDATE LIBRARY (обновление библиотеки)

Определение всех накопителей и путей для одной библиотеки

Команда PERFORM LIBACTION служит для конфигурирования одной библиотеки SCSI или виртуальной ленточной библиотеки (VTL) за один шаг.

Об этой задаче

Если вы конфигурируете или изменяете аппаратную среду и должны создать или изменить большое число определений накопителей, это проще делать при помощи команды PERFORM LIBACTION. Можно определить новую библиотеку, а затем определить все накопители и пути к этим накопителям. Или, если у вас есть существующая библиотека, которую вы хотите удалить, можно удалить все существующие накопители и их пути за один шаг.

Параметр PREVIEW позволяет вам посмотреть вывод команд перед тем, как они будут обработаны, чтобы проверить действие, выполняемое ими. Если вы определяете библиотеку, путь к этой библиотеке должен быть уже определен, чтобы можно было использовать параметр PREVIEW. Параметры PREVIEW и DEVICE нельзя использовать совместно.

Команду PERFORM LIBACTION можно использовать только для библиотек SCSI и VTL. Если вы определяете накопители и пути для библиотеки, нужно, чтобы поддерживалась и была включена опция SANDISCOVERY. У ленточной библиотеки должна быть возможность возвратить адрес, связанный с серийным номером накопителя.

Процедура

Чтобы сконфигурировать библиотеку VTL под именем ODIN, выполните следующие действия:

1. Задайте библиотеку.

   ```
   define library odin libtype=vtl
   ```

2. Определите два накопителя и их пути для вашей новой библиотеки ODIN.
    Операционные системы AIX

```
perform libaction odin action=define device=/dev/lb3 prefix=dr
```

После этого сервер выполнит следующие команды:

```
define path tsmserver odin srct=server destt=library device=/dev/
 lb3 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
 device=/dev/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
 device=/dev/mt2
```

 Операционные системы Linux

```
perform libaction odin action=define device=/dev/tsmscsi/lb3 prefix=dr
```

После этого сервер выполнит следующие команды:

```
define path tsmserver odin srct=server destt=library device=/dev/tsmscsi/lb3
 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
 device=/dev/tsmscsi/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
 device=/dev/tsmscsi/mt2
```

 Операционные системы Windows

```
perform libaction odin action=define device=lb0.0.0.2 prefix=dr
```

После этого сервер выполнит следующие команды:

```
define path tsmserver odin srct=server destt=library device=lb0.0.0.2
 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
 device=mt0.1.0.2 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
 device=mt0.2.0.2
```

Ссылки, связанные с данной:
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (Задать путь, когда пунктом назначения является накопитель)
PERFORM LIBACTION (Задать или удалить все накопители и пути для библиотеки)

Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с одним типом накопителей

Конфигурирование библиотеки VTL или SCSI, содержащей два ленточных накопителя LTO.

Об этой задаче

Эта процедура является примером конфигурирования автоматизированной библиотеки SCSI, содержащей два накопителя в системе сервера. Эта библиотека не используется совместно ни с какими другими серверами или агентами хранения IBM Spectrum Protect и, как правило, подключается к компьютеру-серверу с использованием кабелей SCSI.

В этой конфигурации оба накопителя в библиотеке одного типа устройств. Определите один класс устройств. Для библиотек SCSI и VTL процедура одинакова, за исключением шага определения библиотеки. Для библиотек SCSI определите библиотеку при помощи libtype=scsi. Для библиотек VTL определите библиотеку при помощи libtype=vtl.

Процедура

1. Задайте библиотеку SCSI с именем AUTODLTLIB.

   ```
   define library autoltolib libtype=scsi
   ```

   Если у библиотеки есть устройство чтения штрих-кодов и вы хотите автоматически помечать ленты перед регистрацией в библиотеке, можно задать для параметра AUTOLABEL значение YES. Например:

   ```
   define library autoltolib libtype=scsi autolabel=yes
   ```

2. Задайте для сервера путь к библиотеке.
   Операционные системы AIX

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=/dev/lb3
   ```

   Операционные системы Linux

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=/dev/tsmscsi/lb3
   ```

   Операционные системы Windows

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=lb0.0.0.3
   ```

3. Определите накопители в библиотеке: Оба накопителя принадлежат библиотеке AUTODLTLIB.

   ```
   define drive autoltolib drive01
   define drive autoltolib drive02
   ```

   Совет: Команду PERFORM LIBACTION можно использовать для определения накопителей и нутей для библиотеки в один шаг.
4. Задайте для сервера путь к каждому накопителю.
   Операционные системы AIX

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=/dev/mt4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=/dev/mt5
   ```

   Операционные системы Linux

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=/dev/tsmscsi/mt4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=/dev/tsmscsi/mt5
   ```

   Операционные системы Windows

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=mt0.0.0.4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=mt0.0.0.5
   ```

   Если при определении накопителя не был указан адрес элемента, сервер отправит запрос библиотеке, чтобы получить адрес по умолчанию.

5. Определите класс устройств с именем AUTODLT_CLASS для двух накопителей в библиотеке AUTODLTLIB.

   ```
   define devclass autolto_class library=autodltlib devtype=lto
   ```

6. Определите пул хранения с именем AUTOLTO_POOL, связанный с классом устройств с именем AUTOLTO_CLASS.

   ```
   define stgpool autolto_pool autolto_class maxscratch=20
   ```

7. Пометка и включение библиотечных томов.

   ```
   label libvolume autoltolib search=yes labelsource=barcode checkin=scratch
   ```

8. Выполните проверку созданных определений с помощью следующих команд:

   ```
   query library
   query drive
   query path
   query devclass
   query stgpool
   query libvolume
   ```

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)
DEFINE LIBRARY (Задать библиотеку)
DEFINE PATH (Задать путь, когда пунктом назначения является накопитель)

Пример: Конфигурирование библиотеки SCSI или виртуальной ленточной библиотеки с несколькими типами накопителей

Вы можете сконфигурировать библиотеку с накопителями нескольких типов, например, библиотеку StorageTek L40, содержащую один накопитель DLT и один накопитель LTO Ultrium.

Об этой задаче

Эта процедура является примером конфигурирования автоматизированной библиотеки SCSI, содержащей два накопителя в системе сервера. Эта библиотека не используется совместно ни с какими другими серверами или агентами хранения IBM Spectrum Protect и, как правило, подключается к компьютеру-серверу с использованием кабелей SCSI.

В этой конфигурации у накопителей разные типы устройств. Определите класс устройств для каждого типа накопителей. Накопители различных типов поддерживаются одной библиотекой, если для каждого типа накопителя определен собственный класс устройств. Если конфигурирование выполняется таким способом, необходимо включить определенный формат для типа накопителя, используя для параметра FORMAT любое значение, кроме DRIVE.

Для библиотек SCSI и VTL процедура одинакова, за исключением шага определения библиотеки. Для библиотек SCSI определите библиотеку при помощи libtype=scsi. Для библиотек VTL определите библиотеку при помощи libtype=vtl.

Процедура

1. Определите библиотеку SCSI с именем MIXEDLIB.

   ```
   define library mixedlib libtype=scsi
   ```

2. Задайте для сервера путь к библиотеке.
    Операционные системы AIX

   ```
   define path server1 mixedlib srctype=server desttype=library
   device=/dev/lb3
   ```

    Операционные системы Linux

   ```
   define path server1 mixedlib srctype=server desttype=library
   device=/dev/tsmscsi/lb3
   ```

    Операционные системы Windows

   ```
   define path server1 mixedlib srctype=server desttype=library
   device=lb0.0.0.3
   ```

3. Определите накопители в библиотеке. Оба накопителя принадлежат библиотеке MIXEDLIB.

   ```
   define drive mixedlib dlt1
   define drive mixedlib lto1
   ```

4. Задайте для сервера путь к каждому накопителю. В параметре DEVICE указывается имя драйвера устройства для накопителя, которое является именем специального файла устройства.
    Операционные системы AIX

   ```
   define path server1 dlt1 srctype=server desttype=drive
   library=mixedlib device=/dev/mt4
   define path server1 lto1 srctype=server desttype=drive
   library=mixedlib device=/dev/mt5
   ```

    Операционные системы Linux

   ```
   define path server1 dlt1 srctype=server desttype=drive
   library=mixedlib device=/dev/tsmscsi/mt4
   define path server1 lto1 srctype=server desttype=drive
   library=mixedlib device=/dev/tsmscsi/mt5
   ```

    Операционные системы Windows

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=mt0.0.0.4
   ```

```
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.5
```

Если при определении накопителя не был указан адрес элемента, сервер отправит запрос библиотеке, чтобы получить эти данные.

5. Определите классы устройств.
   Важное замечание: Не используйте формат DRIVE, указанный по умолчанию. Поскольку накопители принадлежат к разным типам, сервер использует функцию спецификации формата для выбора накопителя. Использование формата DRIVE в смешанной библиотеке накопителей может привести к непредсказуемым результатам.

   ```
   define devclass dlt_class library=mixedlib devtype=dlt format=dlt40
   define devclass lto_class library=mixedlib devtype=lto format=ultriumc
   ```

6. Определите пулы хранения, связанные с классами устройств.

   ```
   define stgpool lto_pool lto_class maxscratch=20
   define stgpool dlt_pool dlt_class maxscratch=20
   ```

7. Пометка и включение библиотечных томов.

   ```
   label libvolume mixedlib search=yes labelsource=barcode checkin=scratch
   ```

8. Выполните проверку созданных определений с помощью следующих команд:

   ```
   query library
   query drive
   query path
   query devclass
   query stgpool
   query libvolume
   ```

Защита файл-серверов NAS

Вы можете сконфигурировать и управлять средой резервного копирования, которая защищает файл-сервер NAS (Network-Attached Storage).

Для резервного копирования и восстановления файл-сервера NAS можно использовать сервер IBM Spectrum Protect, клиент резервного копирования и архивирования IBM Spectrum Protect или IBM Spectrum Protect Snapshot, как описано в следующей таблице.

Продукт	**Описание**
Сервер IBM Spectrum Protect	Чтобы производить резервное копирование и восстановление файл-сервера NAS с использованием сервера IBM Spectrum Protect, у вас должен быть установлен продукт IBM Spectrum Protect Extended Edition. Сервер IBM Spectrum Protect можно сконфигурировать для использования сетевого протокола управления данными (NDMP) для резервного копирования и восстановления данных, как описано в следующих темах в этом разделе. Чтобы защитить большие файловые системы NetApp, можно также сконфигурировать IBM Spectrum Protect для использования NetApp SnapMirror to Tape (эта функция также называется SMTape). Функция SnapMirror to Tape использует для резервного копирования копию данных на уровне блоков, что быстрее, чем традиционное полное резервное копирование NDMP, и может применяться, если полное резервное копирование NDMP является непрактичным. Информацию об использовании функции SnapMirror to Tape для резервного копирования и восстановления данных смотрите в разделе Операции резервного копирования и восстановления с использованием функции NetApp SnapMirror to Tape.
Клиент резервного копирования и архивирования IBM Spectrum Protect	Клиент резервного копирования и архивирования можно сконфигурировать для резервного копирования и восстановления данных файл-сервера с использованием протокола Network File System (NFS) или Common Internet File System (CIFS). Информацию об использовании клиента резервного копирования и архивирования для резервного копирования и восстановления данных смотрите в разделе Резервное копирование и восстановление данных с помощью клиентов резервного копирования и архивирования.

Продукт	Описание
IBM Spectrum Protect Snapshot	IBM Spectrum Protect Snapshot можно использовать для резервного копирования и восстановления данных файл-сервера с использованием расширенных технологий снимков в системах хранения. Информацию об использовании IBM Spectrum Protect Snapshot для резервного копирования и восстановления данных смотрите в разделе IBM Spectrum Protect Snapshot для UNIX и Linux - Обзор или IBM Spectrum Protect Snapshot for VMware - Обзор.

- Требования NDMP
  Чтобы использовать операции NDMP для файл-серверов NAS, у вас должен быть установлен компонент IBM Spectrum Protect Extended Edition, и среда файл-сервера должна отвечать определенным требованиям.
- Управление операциями NDMP
  Существует ряд административных действий по управлению операциями NDMP.
- Конфигурирование IBM Spectrum Protect для выполнения операций NDMP
  Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования и восстановления данных на файл-серверах NAS, используя NDMP. Процедура конфигурирвания зависит от того, собираетесь ли вы создавать резервные копии данных с некластеризованного или кластеризованного файл-сервера NAS.
- Резервное копирование и восстановление файл-серверов NAS с использованием NDMP
  После того как вы сконфигурируете IBM Spectrum Protect для выполнения операций NDMP, вы будете готовы к тому, чтобы использовать NDMP.
- Резервное копирование и восстановление на уровне файлов для операций NDMP
  Когда вы производите резервное копирование данных с использованием NDMP, вы можете указать, что сервер IBM Spectrum Protect собирает и сохраняет информацию на уровне файлов в содержании (TOC).
- Операции резервного копирования и восстановления на уровне каталогов
  Если используется большая файловая система NAS, резервное копирование на уровне каталогов позволит сократить время выполнения резервного копирования и восстановления и обеспечит больше гибкости при конфигурировании резервного копирования NAS. Путем определения виртуальных файловых пространств резервное копирование файловой системы можно разделить между несколькими операциями резервного копирования с помощью NDMP и несколькими ленточными накопителями. Также можно использовать различные расписания для резервного копирования поддеревьев файловой системы.
- Операции резервного копирования и восстановления с использованием функции NetApp SnapMirror to Tape
  Можно создать резервные копии больших файловых систем NetApp при помощи функции NetApp SnapMirror to Tape (она также называется SMTape). За счет использования при резервном копировании копии данных на уровне блоков, метод SnapMirror to Tape обеспечивает более высокую скорость, чем традиционное полное резервное копирование NDMP (Network Data Management Protocol), и может использоваться в тех случаях, когда полное резервное копирование NDMP является нерациональным.
- Операции резервного копирования NDMP с использованием интегрированных с файл-сервером контрольных точек Celerra
  Когда сервер IBM Spectrum Protect инициирует операцию резервного копирования NDMP на устройстве перемещения данных Celerra, для выполнения резервного копирования большой файловой системы может потребоваться несколько часов. Без интегрированных контрольных точек Celerra все изменения, происходящие в файловой системе, будут записаны в резервную копию образа.
- Репликация узлов NAS
  Вы можете реплицировать узел NAS, для которого используется NDMP при выполнении операций резервного копирования. Прежде чем конфигурировать операцию репликации, прочтите информацию о действующих ограничениях.

Требования NDMP

Чтобы использовать операции NDMP для файл-серверов NAS, у вас должен быть установлен компонент IBM Spectrum Protect Extended Edition, и среда файл-сервера должна отвечать определенным требованиям.

файл-сервер NAS (NAS file server)

Операционная система файл-сервера должна поддерживаться сервером IBM Spectrum Protect. Информацию о поддерживаемых файл-серверах NAS смотрите в разделе техническое замечание 1054144.

Комбинация модели файл-сервера и операционной системы должна поддерживаться файл-сервером NAS. Дополнительные сведения смотрите в информации о продукте для файл-сервера NAS.

Ленточные библиотеки

Это требование необходимо только при резервном копировании на локально подключенное устройство NAS.
Сервер IBM Spectrum Protect поддерживает следующие типы библиотек для операций, использующих NDMP:

SCSI
: Библиотеку SCSI можно подключить непосредственно к серверу IBM Spectrum Protect или к файл-серверу NAS. При подключении библиотеки непосредственно к серверу IBM Spectrum Protect этот сервер управляет операциями библиотеки, передавая команды SCSI непосредственно библиотеке. При подключении библиотеки непосредственно к файл-серверу NAS сервер IBM Spectrum Protect управляет библиотекой, направляя команды SCSI библиотеке через файл-сервер NAS.

ACSLS
: Библиотеку автоматизированной программы системы картриджей (automated cartridge system library software, ACSLS) можно подключить только непосредственно к серверу IBM Spectrum Protect. Сервер IBM Spectrum Protect управляет библиотекой, направляя запрос к ней через сервер управления библиотекой по протоколу TCP/IP.
Ограничение: Сервер IBM Spectrum Protect не включает в себя поддержку внешних библиотек для библиотеки ACSLS, если она используется для операций NDMP.

VTL
: Виртуальную ленточную билиотеку (virtual tape library, VTL) можно подключить непосредственно к серверу IBM Spectrum Protect или к файл-серверу NAS. Виртуальная ленточная библиотека похожа на библиотеку SCSI, но она оптимизирована для характеристик виртуальной ленточной библиотеки и обеспечивает лучшую производительность монтирования.
Если вы задаете VTL, в вашей среде не должно быть смешанных носителей. Должны быть заданы пути между всеми накопителями в библиотеке и всеми заданными серверами, включая агенты хранения, использующими библиотеку. Если эти условия не выполнены, общая производительность может снизиться до того же уровня, как в случае библиотеки типа SCSI, особенно при высокой нагрузке.

349X;
: Библиотеку 349X можно подключить только непосредственно к серверу IBM Spectrum Protect. Сервер IBM Spectrum Protect управляет библиотекой, направляя запрос к ней через менеджер библиотеки по протоколу TCP/IP.

Совместное использование библиотек: Сервер IBM Spectrum Protect, выполняющий операции NDMP, может быть менеджером библиотеки для библиотеки ACSLS, SCSI, VTL или 349X, но не может быть клиентом библиотеки. Сервер IBM Spectrum Protect также может быть клиентом библиотеки в конфигурации, когда файл-сервер NAS отправляет данные не в ленточную библиотеку, подключенную к файл-серверу NAS, а на сервер с использованием TCP/IP. Если сервер IBM Spectrum Protect, выполняющий операции NDMP, является менеджером библиотеки, он должен непосредственно управлять ею, а не направлять команды через файл-сервер NAS.

Ленточные накопители
: Ленточный накопитель требуется только для резервного копирования на локально подключенное устройство NAS. Файл-сервер NAS должен иметь доступ к накопителям. Устройство NAS не поддерживаются в библиотеке со смешанными типами устройств. Для выполнения операций резервного копирования накопители должны поддерживаться файл-сервером NAS и его операционной системой. Полные сведения о поддержке протоколом NDMP устройств содержатся в документации к файл-серверу NAS.
Совместное использование накопителей: Ленточные накопители могут совместно использоваться сервером IBM Spectrum Protect и одним или несколькими файл-серверами NAS. Кроме того, если библиотека SCSI, VTL или 349X подключена к серверу, а не к файл-серверу NAS, накопители могут совместно использоваться одним или несколькими файл-серверами NAS. Накопители также могут совместно использоваться одним или несколькими клиентами библиотеки IBM Spectrum Protect и агентами хранения.
Резервирование накопителей: Если ленточные накопители подключены к устройствам NAS и в команде DEFINE LIBRARY задан параметр RESETDRIVES=YES, то применяются следующие ограничения:

- Если ленточный накопитель совместно используется сервером IBM Spectrum Protect и устройством NAS, то поддерживается приоритетное прерывание резервирования, если устройство NAS поддерживает постоянное резервирование и оно разрешено. Более подробную информацию о том, как задать постоянное резервирование, смотрите в документации по вашему устройству NAS.
- Если ленточный накопитель подключен только к устройству NAS и не используется совместно с сервером IBM Spectrum Protect, то приоритетное прерывание резервирования не поддерживается. Если вы включите постоянное резервирование на устройстве NAS для этих накопителей, а резервирование задано устройством NAS, но его очистка никогда не производится, вы должны использовать другой метод для очистки резервирования.

Проверьте у производителей оборудования совместимость определенных комбинаций файл-сервера NAS, ленточных накопителей и устройств, подключенных по сети SAN.

Совет: Сервер IBM Spectrum Protect поддерживает NDMP версии 4 для всех операций NDMP. Сервер IBM Spectrum Protect поддерживает все операции резервного копирования и восстановления NDMP с устройством NAS, работающим по протоколу NDMP версии 3. При установлении соединения NDMP с сервером NDMP сервер IBM Spectrum Protect будет использовать наивысший уровень протокола (либо версии 3, либо версии 4). Если при использовании версии 4 возникают неполадки, можно попробовать воспользоваться версией 3.

- Интерфейсы для операций NDMP
  Для выполнения операций NDMP можно использовать несколько интерфейсов. Операцию NDMP можно запланировать с помощью команды BACKUP NODE или RESTORE NODE и создав расписание для обработки команды.
- Форматы данных для операций резервного копирования NDMP
  Данные, резервное копирование которых производится с использованием NDMP, будут представлены не в таком формате, как данные, используемые для обычных операций резервного копирования IBM Spectrum Protect. Файл-сервер NAS управляет форматом данных резервных копий.
- Типы пулов хранения при выполнении операций NDMP
  Прежде чем конфигурировать IBM Spectrum Protect для выполнения операций с использованием сетевого протокола управления данными (network data management protocol, NDMP), узнайте о поддерживаемых типах пулов хранения. Для операций NDMP поддерживаются различные типы пула хранения поддерживаются, в зависимости от бренда файлового сервера, который вы используете.

Интерфейсы для операций NDMP

Для выполнения операций NDMP можно использовать несколько интерфейсов. Операцию NDMP можно запланировать с помощью команды BACKUP NODE или RESTORE NODE и создав расписание для обработки команды.

Интерфейсы клиента:

- Клиент резервного копирования и архивирования для командной строки IBM Spectrum Protect (для систем Windows, 64-разрядной AIX или 64-разрядной Oracle Solaris)
- Интерфейс веб-клиента IBM Spectrum Protect, который поставляется вместе с клиентом резервного копирования-архивирования версии 8.1.1 или более ранней версии

Ограничение: Если вы установили клиент резервного копирования-архивирования V8.1.1 или ранее, то можно использовать интерфейс веб-клиента для операций восстановления уровня файла. Если вы установили клиент резервного копирования-архивирования V8.1.2 или новее, то использовать интерфейс веб-клиента для операций восстановления уровня файла нельзя.
Интерфейсы сервера:

- На консоль сервера
- Командная строка клиента администрирования
  Совет: Во всех примерах для операций NDMP используются серверные команды.

В интерфейсе веб-клиента версии V8.1.1 или более ранней версии показаны файловые системы файл-сервера NAS в графическом представлении. Данная функция клиента не обязательна, но может использоваться для операций с использованием протокола NDMP. При выполнении операций на уровне файлов предпочтительным методом является использование интерфейса веб-клиента V8.1.1 или более ранней версии. Дополнительные сведения об операциях восстановления на уровне файлов смотрите в разделе Резервное копирование и восстановление на уровне файлов для операций NDMP.

При выполнении операций NDMP с использованием любого из интерфейсов клиента сервер IBM Spectrum Protect запросит у вас ID администратора и пароль. Дополнительную информацию об установке и активации интерфейса клиента смотрите в разделе Установка клиентов резервного копирования и архивирования IBM Spectrum Protect.

Чтобы использовать клиент резервного копирования и архивирования или веб-клиент IBM Spectrum Protect для операций NAS, имена файловой системы на устройстве NAS должны начинаться с обычной косой черты (/) в качестве первого символа. Это ограничение не касается операций NAS, инициируемых из командной строки сервера IBM Spectrum Protect.

Форматы данных для операций резервного копирования NDMP

Данные, резервное копирование которых производится с использованием NDMP, будут представлены не в таком формате, как данные, используемые для обычных операций резервного копирования IBM Spectrum Protect. Файл-сервер NAS управляет форматом данных резервных копий.

Данные, резервное копирование которых производится в библиотеку, непосредственно подключенную к файл-серверу, должны быть направлены в пул хранения с нужным форматом данных. Когда вы задаете пул хранения для операций NDMP, вы задаете один из следующих форматов данных:

- NETAPPDUMP, если файл-сервер NAS представляет собой устройством NetApp или IBM® System Storage N Series.
- CELERRADUMP, если файл-сервер NAS является устройством EMC Celerra.
- NDMPDUMP для всех остальных устройств.

Данные, резервное копирование которых производится по сети в локальную иерархию IBM Spectrum Protect, можно направить в любой пул хранения с произвольным доступом или с последовательным доступом. Однако формат данных не изменится.

Типы пулов хранения при выполнении операций NDMP

Прежде чем конфигурировать IBM Spectrum Protect для выполнения операций с использованием сетевого протокола управления данными (network data management protocol, NDMP), узнайте о поддерживаемых типах пулов хранения. Для операций NDMP поддерживаются различные типы пула хранения поддерживаются, в зависимости от бренда файлового сервера, который вы используете.

Операции резервного копирования

Следующие типы пулов хранения могут использоваться для операций резервного копирования.

Бренд файлового сервера	**Можно ли использовать пулы хранения каталогов-контейнеров в качестве места назначения?**	**Можно ли использовать пулы хранения облачных контейнеров в качестве места назначения?**	**Можно ли использовать не дедуплицированные неконтейнерные пулы хранения в качестве места назначения?**	**Можно ли использовать дедуплицированные неконтейнерные пулы хранения типа FILE в качестве места назначения?**
NetApp без использования функции SnapMirror to Tape	Да	Да	Да	Да
NetApp с использованием функции SnapMirror to Tape	Нет	Нет	Да	Нет
Другие бренды	Нет	Нет	Да	Нет

Операции репликации: ограничения для исходных пулов хранения

На исходном сервере при выполнении операций репликации можно использовать следующие типы пулов хранения:

Бренд файлового сервера	**Можно ли использовать пулы хранения каталогов-контейнеров на исходном сервере репликации?**	**Можно ли использовать пулы хранения облачных контейнеров на исходном сервере репликации?**	**Можно ли использовать пулы хранения без контейнеров и без дедупликации на исходном сервере репликации?**	**Можно ли использовать пулы хранения без контейнеров с дедупликацией типа FILE на исходном сервере репликации?**
NetApp без использования функции SnapMirror to Tape	Нет	Нет	Да	Нет
NetApp с использованием функции SnapMirror to Tape	Нет	Нет	Да	Нет

Бренд файлового сервера	Можно ли использовать пулы хранения каталогов-контейнеров на исходном сервере репликации?	Можно ли использовать пулы хранения облачных контейнеров на исходном сервере репликации?	Можно ли использовать пулы хранения без контейнеров и без дедупликации на исходном сервере репликации?	Можно ли использовать пулы хранения без контейнеров с дедупликацией типа FILE на исходном сервере репликации?
Другие бренды	Нет	Нет	Да	Нет

Операции репликации: ограничения для пулов хранения назначения

На сервере репликации назначения можно использовать следующие типы пулов хранения:

Бренд файлового сервера	Можно ли использовать пулы хранения каталогов-контейнеров на сервере репликации назначения?	Можно ли использовать пулы хранения облачных контейнеров на сервере репликации назначения?	Можно ли использовать пулы хранения без контейнеров и без дедупликации на сервере репликации назначения?	Можно ли использовать пулы хранения без контейнеров с дедупликацией типа FILE на сервере репликации назначения?
NetApp без использования функции SnapMirror to Tape	Да	Да	Да	Да
NetApp с использованием функции SnapMirror to Tape	Нет	Нет	Да	Нет
Другие бренды	Нет	Нет	Да	Нет

Операции защиты с записью в удаленный пул хранения

На сервере репликации назначения для защиты данных в пулах хранения каталогов-контейнеров с помощью команды PROTECT STGPOOL можно использовать следующие типы пулов хранения.

Бренд файл-сервера	Можно ли использовать пулы хранения каталогов-контейнеров в качестве места назначения?	Можно ли использовать пулы хранения облачных контейнеров в качестве места назначения?	Можно ли использовать не дедуплицированные неконтейнерные пулы хранения в качестве места назначения?	Можно ли использовать дедуплицированные неконтейнерные пулы хранения типа FILE в качестве места назначения?
NetApp без использования функции SnapMirror to Tape	Да	Н/П	Н/П	Н/П
NetApp с использованием функции SnapMirror to Tape	Нет	Н/П	Н/П	Н/П
Другие бренды	Нет	Н/П	Н/П	Н/П

Операции защиты с записью на ленту на том же сервере

Ниже перечислены типы пулов хранения, которые можно использовать при вводе команды PROTECT STGPOOL для защиты пула хранения каталога-контейнера на ленте на том же сервере.

Бренд файлового сервера	Можно ли использовать пулы хранения каталогов-контейнеров в качестве места назначения?	Можно ли использовать пулы хранения облачных контейнеров в качестве места назначения?	Можно ли использовать не дедуплицированные неконтейнерные пулы хранения в качестве места назначения?	Можно ли использовать дедуплицированные неконтейнерные пулы хранения типа FILE в качестве места назначения?
NetApp без использования функции SnapMirror to Tape	Да	Н/П	Н/П	Н/П
NetApp с использованием функции SnapMirror to Tape	Нет	Н/П	Н/П	Н/П
Другие бренды	Нет	Н/П	Н/П	Н/П

Преобразование пулов хранения

Если данные NDMP существуют в пуле хранения, преобразованном в пул хранения каталога-контейнер или пул хранения облачного контейнера, данные NDMP остаются в исходном пуле хранения и не преобразовываются.

Разбиение на уровни с использованием облака

Если данные NDMP существуют в пуле хранения, разбитом на уровни для хранения облачных объектов, данные NDMP остаются в исходном пуле хранения и не подразделяются на уровни.

Когда NETAPPDUMP, CELERRADUMP или NDMPDUMP определяются как тип пула хранения, ограничения также применяются. Дополнительные сведения смотрите в разделе Управление пулами хранения при выполнении операций NDMP.

Управление операциями NDMP

Существует ряд административных действий по управлению операциями NDMP.

- Управление узлами файл-серверов NAS
  Узлы файл-сервера NAS можно обновлять, переименовывать и удалять и можно запрашивать информацию о них.
- Управление средствами перемещения данных, используемыми в операциях NDMP
  Вы можете запрашивать, обновлять и удалять средства перемещения данных, заданные вами для файл-серверов NAS.
- Как выделить накопитель IBM Spectrum Protect для выполнения операций NDMP
  Если накопитель уже используется для операций IBM Spectrum Protect, его можно использовать для операций NDMP.
- Управление пулами хранения при выполнении операций NDMP
  Когда NETAPPDUMP, CELERRADUMP или NDMPDUMP назначены как тип пула хранения, управление пулами хранения, созданными операциями NDMP, отличается от управления пулами хранения, содержащими носители для традиционных резервных копий IBM Spectrum Protect.
- Управление таблицами содержания
  Существует ряд команд, позволяющих управлять разными характеристиками содержания (Table of Contents, TOC).
- Предотвращение закрытия долгосрочных неактивных соединений NDMP
  Чтобы брандмауэры не закрывали соединения NDMP, которые являются долгосрочными и неактивными, можно включить сигнал активности TCP для управляющих соединений NDMP.

Управление узлами файл-серверов NAS

Узлы файл-сервера NAS можно обновлять, переименовывать и удалять и можно запрашивать информацию о них.

Процедура

Используйте для управления узлами файл-сервера NAS одну из следующих команд:

Команда	Процедура
QUERY NODE	Чтобы запросить информацию об узле, введите команду QUERY NODE с соответствующими параметрами. Например, если вы хотите запросить информацию об узле NAS NASNODE1, введите следующую команду: `query node nasnode1 type=nas`
UPDATE NODE	Чтобы обновить узел, введите команду UPDATE NODE с соответствующими параметрами. Например, если вы создали новый домен политики с именем NASDOMAIN для узлов NAS и хотите обновить узел NASNODE1, включив узел в новый домен, введите следующую команду: `update node nasnode1 domain=nasdomain`
RENAME NODE	Чтобы переименовать узел NAS, нужно также переименовать соответствующее устройство перемещения данных NAS; они должны иметь одно и то же имя. Например, чтобы переименовать узел NASNODE1 в NAS1, выполните следующие действия: 1. Удалить все пути между средством (узлом) перемещения данных NASNODE1 и библиотеками, а также между средством перемещения данных NASNODE1 и накопителями. 2. Удалить узел перемещения данных, заданный для узла NAS. 3. Чтобы переименовать узел NASNODE1 в NAS1, введите следующую команду: `rename node nasnode1 nas1` 4. Задайте узел перемещения данных, используя новое имя узла. В этом примере необходимо задать новый узел перемещения данных с именем NAS1 с теми же параметрами, которые использовались для определения узла NASNODE1. Важное замечание: При определении нового узла перемещения данных для переименованного узла убедитесь, что имя узла перемещения данных совпадает с новым именем узла. Кроме того, убедитесь, что параметры нового узла перемещения данных - это дубликаты параметров первоначального узла перемещения данных. Любое несовпадение между именем узла и именем узла перемещения данных или между параметрами нового и первоначального узла перемещения данных может помешать установке сеанса с файл-сервером NAS. 5. Для библиотек SCSI или 349X определять путь между узлом перемещения данных NAS и библиотекой необходимо, только если библиотека физически подключена непосредственно к файл-серверу NAS. 6. Задайте пути от узла перемещения данных NAS к накопителям, используемым для выполнения операций NDMP.

Команда	Процедура
REMOVE NODE	Чтобы удалить узел, сделайте следующее: 1. Удалите все определения файловых пространств для данного узла. 2. Удалить все пути между средством (узлом) перемещения данных и библиотеками, а также между средством перемещения данных и накопителями. 3. Удалите узел. Например, если вы хотите удалить узел NAS1, введите следующую команду: `remove node nas1`

Ссылки, связанные с данной:
QUERY NODE (Запросить информацию об узлах)
UPDATE NODE (Обновить атрибуты узла)
RENAME NODE (переименование узла)
REMOVE NODE (удаление узла или связанного узла-компьютера)

Управление средствами перемещения данных, используемыми в операциях NDMP

Вы можете запрашивать, обновлять и удалять средства перемещения данных, заданные вами для файл-серверов NAS.

Процедура

Используйте для управления средствами перемещения данных одну из следующих команд:

Команда	Процедура
QUERY DATAMOVER	Чтобы запросить информацию о средстве перемещения данных, введите команду QUERY DATAMOVER с соответствующими параметрами. Например, если вы хотите запросить информацию о средстве перемещения данных NASNODE1, введите следующую команду: `query datamover nasnode1`
UPDATE DATAMOVER	Чтобы обновить средство перемещения данных, введите команду UPDATE DATAMOVER с соответствующими параметрами. Например, если вы завершаете работу файл-сервера NAS для технического обслуживания и хотите перевести средство перемещения данных в отключенный режим, введите следующую команду: `update datamover nasnode1 online=no`
DELETE DATAMOVER	Чтобы удалить средство перемещения данных, введите команду DELETE DATAMOVER. Например, если вы хотите удалить средство перемещения данных NASNODE1, введите следующую команду: `delete datamover nasnode1` Ограничение: Если у устройства перемещения данных есть путь к библиотеке, то при удалении устройства или переводе его в отключенный режим доступ к библиотеке будет отключен.

Ссылки, связанные с данной:
QUERY DATAMOVER (Вывести на экран определения средства перемещения данных)
UPDATE DATAMOVER (Обновить средство перемещения данных)
DELETE DATAMOVER (Удалить средство перемещения данных)

Как выделить накопитель IBM Spectrum Protect для выполнения операций NDMP

Если накопитель уже используется для операций IBM Spectrum Protect, его можно использовать для операций NDMP.

Процедура

Удалите права доступа к серверу IBM Spectrum Protect, удалив определение пути. Например, если имя сервера - SERVER1, а накопителем является NASDRIVE1, введите следующую команду:

```
delete path server1 nasdrive1 srctype=server desttype=drive library=naslib
```

Управление пулами хранения при выполнении операций NDMP

Когда NETAPPDUMP, CELERRADUMP или NDMPDUMP назначены как тип пула хранения, управление пулами хранения, созданными операциями NDMP, отличается от управления пулами хранения, содержащими носители для традиционных резервных копий IBM Spectrum Protect.

Приведенные ниже рекомендации и ограничения относятся к пулам хранения типов NETAPPDUMP, CELERRADUMP и NDMPDUMP, сгенерированных операциями NDMP:

- Пулы хранения можно запрашивать и обновлять, но обновить параметр DATAFORMAT нельзя.
- Задать пул хранения CENTERA, пул хранения каталога-контейнера или пул хранения облачного контейнера в качестве пула назначения для операций NDMP нельзя.
- Наличие отдельных пулов хранения для данных от разных поставщиков NAS является предпочтительной практикой, даже если формат данных в обоих пулах - это NDMPDUMP.
- Следующие параметры команд DEFINE STGPOOL и UPDATE STGPOOL игнорируются, поскольку иерархии, высвобождение носителей и перенос для этих пулов хранения не поддерживаются:
  - MAXSIZE
  - NEXTSTGPOOL
  - LOWMIG
  - HIGHMIG
  - MIGDELAY
  - MIGCONTINUE
  - RECLAIMSTGPOOL
  - OVFLOCATION

Важное замечание: Убедитесь, что вы не используете случайно пулы хранения, определенные для операций NDMP, в традиционных операциях IBM Spectrum Protect. Особая осторожность необходима при присвоении пулу хранения имени в виде значения параметра DESTINATION команды DEFINE COPYGROUP. Если пункт назначения не представляет собой пул хранения с соответствующим форматом данных, резервное копирование завершится неудачно.

Управление таблицами содержания

Существует ряд команд, позволяющих управлять разными характеристиками содержания (Table of Contents, TOC).

Об этой задаче

При помощи команды SET TOCLOADRETENTION можно указать, сколько примерно минут содержание (Table of Contents, TOC), к которому не было обращений в течение этого времени, останется загруженным в базу данных IBM Spectrum Protect. Срок хранения TOC на уровне сервера IBM Spectrum Protect определяет, сколько времени загруженное TOC будет храниться в базе данных после последнего обращения к информации TOC.

Поскольку информация TOC загружается во временные таблицы базы данных, эти данные будут утеряны при остановке сервера, даже если срок хранения TOC еще не истек. При установке время хранения задается равным 120 минутам. Чтобы узнать текущий срок хранения TOC, используйте команду QUERY STATUS.

Чтобы вызвать информацию об объектах образов файловых систем, созданных в ходе резервного копирования того или иного узла NAS и файлового пространства, введите команду QUERY NASBACKUP. Введя эту команду, вы сможете увидеть

все резервные копии образов, сгенерированные в ходе операций NDMP, а также то, есть ли у каждого образа соответствующее содержание (TOC).
Совет: Сервер IBM Spectrum Protect может хранить полную резервную копию свыше указанного количества версий, если имеются зависимые от нее дифференциальные копии. Обработка полных резервных копий NAS с зависимыми дифференциальными копиями тождественна обработке других основных файлов с зависимыми субфайлами. Благодаря заданному при помощи параметра RETEXTRA сроку хранения, полная резервная копия NAS не устареет, а версия будет показана в выходной информации команды QUERY NASBACKUP. Информацию о том, как задать политики хранения данных, смотрите в разделе Настройка политик.

Для просмотра файлов и каталогов образа резервной копии, созданного средствами NDMP, воспользуйтесь командой QUERY TOC. Введя серверную команду QUERY TOC, также можно увидеть все каталоги и файлы в указанном содержании (TOC). Указанное содержание (TOC) читается из пула хранения при каждом вводе команды QUERY TOC, так как эта команда не загружает информацию TOC в базу данных IBM Spectrum Protect. Затем введите команду RESTORE NODE с параметром FILELIST, чтобы восстановить отдельные файлы.

Предотвращение закрытия долгосрочных неактивных соединений NDMP

Чтобы брандмауэры не закрывали соединения NDMP, которые являются долгосрочными и неактивными, можно включить сигнал активности TCP для управляющих соединений NDMP.

Об этой задаче

Сервер IBM Spectrum Protect инициирует управляющие соединения с устройствами NAS во время операций резервного копирования или восстановления NDMP. Эти управляющие соединения могут оставаться открытыми и неактивными в течение длительного времени. Например, предположим, что две операции NDMP начаты для одного устройства NAS. Управляющее соединение для одной операции NDMP может оставаться открытым, но неактивным, если для операции требуется определенный ресурс, например ленточное устройство или последовательный том, который используется другой операцией NDMP.

Некоторые брандмауэры настроены автоматически закрывать сетевые соединения, если они неактивны в течение определенного периода времени. Если между сервером IBM Spectrum Protect и устройством NAS есть брандмауэр, он может неожиданно закрывать управляющие соединения NDMP и вызывать ошибку выполнения операции NDMP.

Сервер IBM Spectrum Protect предоставляет механизм - сигнал активности TCP, который можно использовать для предотвращения закрытия долгосрочных неактивных соединений. Когда функция сигнала активности TCP включена, небольшие пакеты отправляются по сети через определенные интервалы времени второй стороне соединения.

Ограничение: Во избежание ошибок не включайте сигнал активности TCP (keepalive) в некоторых типах сред. Одним из примеров являются среды, в которых нет брандмауэров между сервером IBM Spectrum Protect и устройством NAS. Другим примером являются среды с брандмауэрами, допускающими длительно работающие неактивные соединения. Если включить поддержку сигнала активности TCP в средах такого типа, это может привести к нежелательному закрытию бездействующего соединения, когда партнер соединения временно не сможет отвечать на пакеты сигнала активности TCP.

- Включение сигнала активности TCP (keepalive)
  Чтобы включить сигнал активности TCP, который сохраняет соединения NDMP открытыми, используют опцию сервера NDMPENABLEKEEPALIVE.
-  Операционные системы AIX  Операционные системы LinuxОперационные системы WindowsЗадание времени бездействия соединения для сигнала активности TCP
  Задать время бездействия соединения в минутах до отправки первого пакета сигнала активности TCP можно при помощи опции сервера NDMPKEEPIDLEMINUTES.

Включение сигнала активности TCP (keepalive)

Чтобы включить сигнал активности TCP, который сохраняет соединения NDMP открытыми, используют опцию сервера NDMPENABLEKEEPALIVE.

Процедура

Добавьте опцию в файл опций сервера dsmserv.opt:

```
ndmpenablekeepalive yes
```

Ссылки, связанные с данной:
NDMPENABLEKEEPALIVE
Операционные системы AIXОперационные системы LinuxОперационные системы Windows

Задание времени бездействия соединения для сигнала активности TCP

Задать время бездействия соединения в минутах до отправки первого пакета сигнала активности TCP можно при помощи опции сервера NDMPKEEPIDLEMINUTES.

Процедура

Добавьте опцию в файл опций сервера dsmserv.opt:

```
ndmpkeepidleminutes число_минут
```

Ссылки, связанные с данной:
NDMPKEEPIDLEMINUTES

Конфигурирование IBM Spectrum Protect для выполнения операций NDMP

Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования и восстановления данных на файл-серверах NAS, используя NDMP. Процедура конфигурирвания зависит от того, собираетесь ли вы создавать резервные копии данных с некластеризованного или кластеризованного файл-сервера NAS.

Прежде чем начать

Ознакомьтесь с ограничениями на операции резервного копирования NDMP:

- Дедупликация данных поддерживается только при работе с файл-серверами NetApp, не использующими функцию SnapMirror to Tape.
- Пулы хранения контейнеров поддерживаются только при работе с файл-серверами NetApp, не использующими функцию SnapMirror to Tape.

Дополнительную информацию о типах пулов хранения, которые поддерживаются для различных брендов файловых серверов, смотрите в разделе Типы пулов хранения при выполнении операций NDMP.

- Конфигурирование IBM Spectrum Protect для операций NDMP в некластеризованной среде
  Чтобы использовать IBM Spectrum Protect для выполнения операций с использованием сетевого протокола управления данными (network data management protocol, NDMP) в некластеризованной среде, нужно настроить ленточную библиотеку и носители и выполнить дополнительные шаги по конфигурированию.
- Конфигурирование IBM Spectrum Protect для операций NDMP в кластеризованной среде NetApp
  Вы можете производить резервное копирование данных из кластера NetApp на непосредственно подключенное ленточное устройство или на сервер IBM Spectrum Protect, который хранит данные в пуле хранения. Можно создать резервную копию всего кластера на одном узле IBM Spectrum Protect или частей кластера на нескольких узлах.

Конфигурирование IBM Spectrum Protect для операций NDMP в некластеризованной среде

Чтобы использовать IBM Spectrum Protect для выполнения операций с использованием сетевого протокола управления данными (network data management protocol, NDMP) в некластеризованной среде, нужно настроить ленточную библиотеку и носители и выполнить дополнительные шаги по конфигурированию.

Прежде чем начать

1. Ознакомьтесь с ограничениями на операции NDMP:

- Чтобы сконфигурировать IBM Spectrum Protect для выполнения операций NDMP в некластеризованной среде, следует использовать устройство сетевого хранилища данных (network-attached storage, NAS), возможность использования которого в сочетании с IBM Spectrum Protect была проверена при помощи программы проверки Ready for IBM®.
- Операции дедупликации данных и пулы хранения контейнеров поддерживаются только файл серверами NetApp, которые не используют функцию SnapMirror to Tape. Все остальные устройства NAS, проверенные на возможность использования в сочетании с IBM Spectrum Protect в соответствии с программой проверки Ready for IBM, должны использовать недедуплицированные пулы хранения, не являющиеся пулами хранения контейнеров. Дополнительную информацию о типах пулов хранения, которые поддерживаются для различных брендов файловых серверов, смотрите в разделе Типы пулов хранения при выполнении операций NDMP.

2. Зарегистрируйте лицензию на IBM Spectrum Protect Extended Edition. Чтобы создать резервную копию данных файл-сервера NAS и восстановить эти данные, используя сервер IBM Spectrum Protect, требуется IBM Spectrum Protect Extended Edition.

Процедура

1. Настроить ленточную библиотеку и носители информации. Дополнительные сведения о следующих шагах смотрите в разделе Конфигурирование ленточной библиотеки для операций NDMP.
   a. Подключить библиотеку SCSI или виртуальную ленточную библиотеку (VTL) к файл-серверу NAS или к серверу IBM Spectrum Protect, или подключить библиотеку ACSLS или библиотеку 349X к серверу IBM Spectrum Protect.
   b. Определить библиотеку с типом SCSI, VTL, ACSLS или 349X.
   c. Определить класс устройства для ленточных накопителей.
   d. Определить пул хранения для резервных носителей NAS.
   e. Необязательно: Определить пул для хранения содержания.
2. Настроить политику сервера IBM Spectrum Protect для управления резервными копиями образов NAS. Смотрите раздел Конфигурирование политики IBM Spectrum Protect для операций NDMP.
3. Зарегистрировать узел файл-сервера NAS на сервере IBM Spectrum Protect. Смотрите раздел Регистрация узлов NAS на сервере IBM Spectrum Protect.
4. Определить устройство перемещения данных для файл-сервера NAS. Смотрите раздел Как задать узел перемещения данных для файл-сервера NAS.
5. Определить путь либо от сервера IBM Spectrum Protect, либо от файл-сервера NAS к библиотеке. Смотрите раздел Определение путей к библиотекам для операций NDMP.
6. Определить ленточные накопители на сервере IBM Spectrum Protect и пути к этим накопителям от файл-сервера NAS и (необязательно) от сервера IBM Spectrum Protect. Смотрите раздел Определение путей для операций NDMP.
7. Зарегистрировать тенты в библиотеке и промаркировать их.

    Операционные системы AIX  Операционные системы LinuxЛенточным томам следует присваивать метки для того, чтобы сервер мог их использовать. Можно использовать команду LABEL LIBVOLUME или параметр AUTOLABEL с командами DEFINE LIBRARY и UPDATE LIBRARY.

    Операционные системы WindowsВсе носители должны иметь метки. При присвоении меток носителям в автоматизированной библиотеке нужно зарегистрировать носители в библиотеке. Чтобы присвоить метки томам при помощи команды LABEL LIBVOLUME, укажите параметры CHECKIN. Чтобы автоматически присваивать метки томам в библиотеках типа SCSI, задайте параметр AUTOLABEL в командах DEFINE LIBRARY и UPDATE LIBRARY.

   Инструкции можно найти в LABEL LIBVOLUME, DEFINE LIBRARY и UPDATE LIBRARY.

8. Необязательно: Настроить резервное копирование по графику для файл-серверов NAS. Смотрите раздел Планирование операций NDMP.
9. Необязательно: Определить имя виртуального файлового пространства. Смотрите раздел Как задать виртуальные файловые пространства.
10. Необязательно: Настройте функцию копирования с ленты на ленту для резервного копирования данных. Смотрите раздел Резервное копирование данных с использованием функции лента-на-ленту.
11. Необязательно: Настройте функцию копирования с ленты на ленту для перемещения данных на другую ленточную технологию. Смотрите раздел Перемещение данных с использованием функции копирования с ленты на ленту.

- Конфигурирование политики IBM Spectrum Protect для операций NDMP
  Используя политики, вы можете управлять числом версий резервных копий образов NDMP и сроком их хранения.
- Ленточные библиотеки и накопители для операций NDMP
  Большая часть работы по планированию, необходимой для выполнения операций резервного копирования и

восстановления с использованием протокола NDMP, относится к конфигурированию устройств. Необходимо выбрать способ подключения и использования библиотек и накопителей.

- Подключение устройств ленточных библиотек при использовании случае библиотек, подключенных к NAS
  Если вы собираетесь создать резервную копию данных NAS в библиотеке, подключенной непосредственно к устройству NAS и используете ленточную библиотеку SCSI, вы должны решить, куда следует подключить библиотеку.
- Регистрация узлов NAS на сервере IBM Spectrum Protect
  Зарегистрируйте файл-сервер NAS в качестве узла IBM Spectrum Protect, указав TYPE=NAS. Это имя узла используется для отслеживания резервных копий образов для файл-сервера NAS.
- Как задать узел перемещения данных для файл-сервера NAS
  Задайте узел перемещения данных для каждого файл-сервера NAS, использующего операции NDMP в вашей среде. Имя узла перемещения данных должно совпадать с именем узла, указанного при регистрации узла NAS на сервере IBM Spectrum Protect.
- Определение путей для операций NDMP
  Для операций NDMP надо создать пути к накопителям и библиотекам.
- Планирование операций NDMP
  Можно запланировать операции резервного копирования или восстановления для изображений, произведенных операциями NDMP. Используйте административные расписания, которые обрабатывают административные команды BACKUP NODE и RESTORE NODE.
- Как задать виртуальные файловые пространства
  Используйте определение виртуального файлового пространства для резервного копирования NAS на уровне каталогов. Для сокращения времени выполнения резервного копирования и восстановления больших файловых систем можно сопоставить путь к каталогу от файл-сервера NAS с именем виртуального файлового пространства на сервере IBM Spectrum Protect.
- Резервное копирование данных с использованием функции лента-на-ленту
  При использовании функции NDMP для копирования с ленты на ленту для резервного копирования данных типом библиотеки может быть SCSI, 349X или ACSLS (automated cartridge system library software). Накопители могут использоваться совместно устройствами NAS и сервером IBM Spectrum Protect.
- Перемещение данных с использованием функции копирования с ленты на ленту
  Чтобы переместить данные с ленточного накопителя, основанного на более старой технологии, на ленточный накопитель, основанный на более новой технологии, используя операцию NDMP копирования с ленты на ленту, вы должны выполнить стандартные шаги по настройке конфигурации, а также дополнительные шаги.

Конфигурирование политики IBM Spectrum Protect для операций NDMP

Используя политики, вы можете управлять числом версий резервных копий образов NDMP и сроком их хранения.

Об этой задаче

Дополнительную информацию смотрите в разделе Политики для резервных копий, инициированные сервером IBM Spectrum Protect.

Процедура

Чтобы сконфигурировать политику для операций NDMP, выполните следующие действия:

1. Создайте домен политики для файл-серверов NAS. К примеру, чтобы определить домен политик с именем NASDOMAIN, введите следующую команду:

   ```
   define domain nasdomain description='Домен политики для файл-серверов NAS'
   ```

2. Создайте в этом домене набор политик. Например, чтобы задать набор политик с именем STANDARD в домене политики NASDOMAIN, введите следующую команду:

   ```
   define policyset nasdomain standard
   ```

3. Задайте класс управления, а затем назначьте его как используемый по умолчанию для набора политик. Например, чтобы задать класс управления MC1 в наборе политик STANDARD и назначить его классом по умолчанию, введите следующие команды:

   ```
   define mgmtclass nasdomain standard mc1
   ```

```
assign defmgmtclass nasdomain standard mc1
```

4. Определите группу резервных копий в используемом по умолчанию классе управления. Конечным расположением должен быть пул хранения, созданный для резервных копий образов, создаваемых операциями NDMP. Кроме того, можно указать количество хранимых версий резервных копий. Например, чтобы задать группу резервных копий для класса управления MC1, который позволяет хранить до четырех версий каждой файловой системы для пула хранения NASPOOL, введите следующую команду:

   ```
   define copygroup nasdomain standard mc1 destination=naspool verexists=4
   ```

   Если вы хотите создать содержание для резервных копий, параметр TOCDESTINATION группы копий должен содержать имя первичного пула хранения.

   ```
   define copygroup nasdomain standard mc1 destination=naspool
   tocdestination=tocpool verexists=4
   ```

   Важное замечание: Задавая группу копий для класса управления, с которым будет связан образ файловой системы, созданный NDMP, убедитесь, что в параметре DESTINATION указано имя пула хранения, определенного для операций NDMP. Если в параметре DESTINATION указан неправильный пул хранения, то при резервном копировании посредством NDMP произойдет ошибка.
5. Активируйте набор политик. Например, чтобы активировать набор политик STANDARD в домене политики NASDOMAIN, введите следующую команду:

   ```
   activate policyset nasdomain standard
   ```

   Политика готова и использованию. Узлы связываются с политикой при регистрации. Дополнительные сведения смотрите в разделе Регистрация узлов NAS на сервере IBM Spectrum Protect.

- Политики для резервных копий, инициированные сервером IBM Spectrum Protect
  Вы можете зарегистрировать файл-сервер NAS (Network-Attached Storage) как узел, используя операцию NDMP (Network Data Management Protocol). По указанию сервера IBM Spectrum Protect файл-сервер NAS производит резервное копирование и восстановление файловой системы и образов каталогов в ленточную библиотеку.
- Политики резервного копирования, инициируемого с помощью интерфейса клиента
  Когда клиентский узел инициирует операцию резервного копирования, политика назначается файлом параметров для данного клиентского узла.
- Определение расположения резервной копии NAS
  Когда IBM Spectrum Protect использует NDMP для защиты файл-серверов NAS, сервер IBM Spectrum Protect управляет операциями. В это время файл-сервер NAS передает данные либо в присоединенную библиотеку, либо непосредственно на сервер IBM Spectrum Protect.

Политики для резервных копий, инициированные сервером IBM Spectrum Protect

Вы можете зарегистрировать файл-сервер NAS (Network-Attached Storage) как узел, используя операцию NDMP (Network Data Management Protocol). По указанию сервера IBM Spectrum Protect файл-сервер NAS производит резервное копирование и восстановление файловой системы и образов каталогов в ленточную библиотеку.

Сервер IBM Spectrum Protect инициирует резервное копирование, выделяет накопитель, выбирает и монтирует носитель. Файл-сервер NAS затем переносит данные на ленту.

Так как файл-сервер NAS создает резервные копии данных, данные хранятся в его собственном формате. Большинство файл-серверов NAS хранят данные в формате NDMPDUMP. Файл-серверы NetApp хранят данные в формате NETAPPDUMP. Файл-серверы EMC хранят данные в формате CELERRADUMP. Для управления резервными копиями образов файл-сервера NAS группы атрибутов копирования для узлов NAS должны указывать на пул хранения, который имеет формат данных NDMPDUMP, NETAPPDUMP или CELERRADUMP.

Следующие атрибуты группы для образов NAS игнорируются:

- Периодичность
- Режим
- Хранить одну версию;
- сериализация;
- Число версий удаленных данных

Чтобы настроить необходимую политику для узлов NAS, можно определить новый, отдельный домен политики.

Когда сервер IBM Spectrum Protect создаст содержание (TOC), вы сможете просмотреть собрание отдельных файлов и каталогов, резервные копии которых были сделаны с использованием NDMP. Затем можно выбрать файлы и каталоги, которые нужно восстановить. Чтобы установить, куда отправлять данные и где хранить содержание (TOC), задайте политику следующим образом:

- Убедитесь, что данные резервной копии образа отправлены в пул хранения формата NDMPDUMP, NETAPPDUMP или CELERRADUMP.
- Убедитесь, что содержание (TOC) отправлено в пул хранения формата NATIVE или NONBLOCK.

Политики резервного копирования, инициируемого с помощью интерфейса клиента

Когда клиентский узел инициирует операцию резервного копирования, политика назначается файлом параметров для данного клиентского узла.

Классами управления, которые применяются к резервным копиям образов, создаваемым операциями NDMP (Network Data Management Protocol), можно управлять независимо от того, какой узел инициирует резервное копирование. Эту задачу можно выполнить, создав набор параметров, используемых клиентскими узлами. Набор параметров может содержать оператор `include.fs.nas` для определения класса управления для операций резервного копирования файл-сервера NAS (Network Attached Storage).

Совет: Набор опций можно задать при помощи команды DEFINE CLOPTSET. Затем добавьте опцию клиента в набор опций с помощью команды DEFINE CLIENTOPT. Набор опций можно назначить для клиента, выполните следующие шаги:

1. Откройте страницу Обзор в центре операций и щелкните по Клиенты.
2. Дважды щелкните по клиенту и выберите Свойства.
3. В поле Набор опций выберите набор опции и нажмите на Сохранить.

Инструкции по использованию команды DEFINE CLOPTSET смотрите в разделе DEFINE CLOPTSET (Определить имя набора опций клиента). Инструкции по использованию команды DEFINE CLIENTOPT смотрите в разделе DEFINE CLIENTOPT (задать опцию для набора опций).

Определение расположения резервной копии NAS

Когда IBM Spectrum Protect использует NDMP для защиты файл-серверов NAS, сервер IBM Spectrum Protect управляет операциями. В это время файл-сервер NAS передает данные либо в присоединенную библиотеку, либо непосредственно на сервер IBM Spectrum Protect.

При помощи клиента резервного копирования и архивирования также можно производить резервное копирование файл-сервера NAS, смонтировав файловую систему NAS на компьютере-клиенте, а затем выполнив резервное копирование как обычно. Можно использовать точку монтирования NFS (Network File System) или карту CIFS (Common Internet File System).

Описание методов резервного копирования и восстановления смотрите в разделе Табл. 1.

Совет: В конкретной среде хранения можно использовать один метод или их комбинацию.

Табл. 1. Сравнение методов резервного копирования данных NDMP

Свойство	NDMP: С файл-сервера на сервер	NDMP: С файл-сервера в подключенную библиотеку	С клиента резервного копирования и архивирования на сервер
Сетевой трафик	Все резервные копии данных передаются по сети с файл-сервера NAS на сервер.	Сервер управляет операциями удаленно, а файл-сервер NAS перемещает данные локально.	Все резервные копии данных передаются по сети с устройства NAS на клиент, а затем на сервер.

Свойство	NDMP: С файл-сервера на сервер	NDMP: С файл-сервера в подключенную библиотеку	С клиента резервного копирования и архивирования на сервер
Обработка данных файл-сервером во время резервного копирования	По сравнению с использованием клиента резервного копирования и архивирования требуется меньше обработки данных файл-сервером, так как при резервном копировании не используются протоколы доступа к файлам, такие как NFS или CIFS.	По сравнению с использованием клиента резервного копирования и архивирования требуется меньше обработки данных файл-сервером, так как при резервном копировании не используются протоколы доступа к файлам, такие как NFS или CIFS.	При выполнении операций резервного копирования файлов для таких протоколов доступа к файлам, как NFS и CIFS, требуется больше ресурсов обработки сервера.
Расстояние между устройствами	Сервер IBM Spectrum Protect должен находиться в пределах доступности по каналу SCSI или волоконно-оптическому каналу от библиотеки лент.	Сервер IBM Spectrum Protect может быть удален от файл-сервера NAS и библиотеки лент.	Сервер IBM Spectrum Protect должен находиться в пределах доступности по каналу SCSI или волоконно-оптическому каналу от библиотеки лент.
Замечания по настройке брандмауэра	Более строгие требования, чем при копировании из библиотеки, подключенной к файл-серверу, так как связь может инициироваться либо сервером IBM Spectrum Protect, либо файл-сервером NAS.	Более низкий уровень безопасности, чем при копировании с файл-сервера на сервер, так как обмен информацией может быть инициирован только сервером IBM Spectrum Protect.	Пароли и данные клиентов шифруются.
Замечания по безопасности	Данные передаются с файл-сервера NAS на сервер IBM Spectrum Protect в расшифрованном виде.	Этот метод следует использовать в доверенной среде, поскольку номера портов не защищены.	Конфигурация портов позволяет проводить безопасные административные сеансы внутри частной сети.
Нагрузка на сервер IBM Spectrum Protect	Управление всеми внутренними процессами обработки данных на сервере (например, переносом) требует более высокой нагрузки на процессор.	Рабочая нагрузка на процессор сокращается, так как перенос данных и высвобождение пространства не поддерживаются.	Управление всеми внутренними процессами обработки данных на сервере требует более высокой нагрузки на процессор.
Резервное копирование первичных пулов хранения в пулы хранения копий	Резервное копирование данных можно выполнять только в пулы хранения копий с форматом данных NATIVE.	Резервное копирование данных можно выполнять только в пулы хранения копий с таким же форматом NDMP-данных (NETAPPDUMP, CELERRADUMP или NDMPDUMP).	Резервное копирование данных можно выполнять только в пулы хранения копий с форматом данных NATIVE.
Восстановление первичных пулов хранения и томов из пулов хранения копий	Данные можно восстанавливать только в пулы хранения и тома с форматом данных NATIVE.	Данные можно восстанавливать только в пулы хранения и тома с тем же форматом NDMP.	Данные можно восстанавливать только в пулы хранения и тома с форматом данных NATIVE.
Перемещение NDMP-данных из томов пулов хранения	Данные можно перемещать в другой пул хранения только в случае, если его формат данных — NATIVE.	Данные можно перемещать в другой пул хранения только в случае, если он имеет такой же формат NDMP-данных.	Данные можно перемещать в другой пул хранения только в случае, если его формат данных — NATIVE.

Свойство	NDMP: С файл-сервера на сервер	NDMP: С файл-сервера в подключенную библиотеку	С клиента резервного копирования и архивирования на сервер
Перенос данных из одного первичного пула хранения в другой	Поддерживается	Не поддерживается	Поддерживается
Освобождение пространства в пуле хранения	Поддерживается	Не поддерживается	Поддерживается
Операции одновременной записи при выполнении резервного копирования	Не поддерживается	Не поддерживается	Поддерживается
Операции экспорта и импорта	Не поддерживается	Не поддерживается	Поддерживается
Создание наборов резервных копий	Не поддерживается	Не поддерживается	Поддерживается
Проверка CRC при перемещении данных с использованием процессов IBM Spectrum Protect	Поддерживается	Не поддерживается	Поддерживается
Проверка с помощью команд аудита IBM Spectrum Protect	Поддерживается	Не поддерживается	Поддерживается
Менеджер аварийного восстановления	Поддерживается	Поддерживается	Поддерживается

Ленточные библиотеки и накопители для операций NDMP

Большая часть работы по планированию, необходимой для выполнения операций резервного копирования и восстановления с использованием протокола NDMP, относится к конфигурированию устройств. Необходимо выбрать способ подключения и использования библиотек и накопителей.

Многие из вариантов настройки библиотек и накопителей определяются возможностями оборудования библиотек. Операции NDMP можно выполнять при любых поддерживаемых библиотеке и накопителях. Однако чем шире возможности библиотеки, тем больше ее гибкость при настройке.

Можно начать с ответов на следующие вопросы:

- Какой тип библиотеки (SCSI, ACSLS, или 349X) планируется использовать?
- Если используется библиотека SCSI, к какому из серверов подключать устройство ленточной библиотеки: IBM Spectrum Protect или файл-серверу NAS (network-attached storage)?
- Нужно ли перемещать данные NDMP на ленту?
- Как использовать ленточные накопители в библиотеке?
    - Выделять ли все ленточные накопители под операции NDMP?
    - Выделить ли часть ленточных накопителей под операции NDMP, а остальные — под традиционные операции IBM Spectrum Protect?
    - Нужно ли совместно использовать ленточные накопители в операциях NDMP и традиционных операциях IBM Spectrum Protect?.
- Создавать ли резервные копии данных с ленты на ленту для аварийного восстановления?
- Создавать ли резервные копии данных на одном сервере IBM Spectrum Protect вместо того, чтобы подключить библиотеку лент к каждому устройству NAS?
- Подключить ли все оборудование к серверу IBM Spectrum Protect и отсылать данные NDMP по локальной сети?

- Определение использования накопителей библиотек при резервном копировании данных в библиотеки, подключенные к NAS
  Благодаря гибкости конфигураций, допускаемых сервером IBM Spectrum Protect, накопители можно использовать для различных целей. Для операций NDMP файл-сервер NAS должен иметь доступ к накопителю. Сервер IBM Spectrum Protect также должен иметь доступ к тому же накопителю в зависимости от подключений и ограничений оборудования.

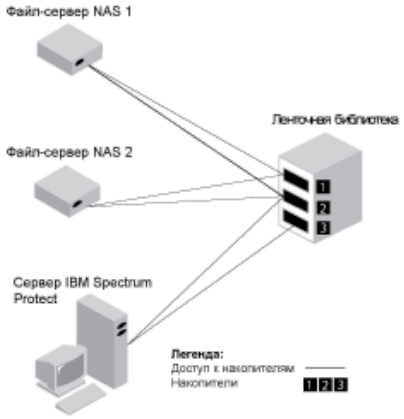
- Конфигурирование ленточной библиотеки для операций NDMP
  Ленточную библиотеку можно сконфигурировать для резервного копирования сетевого устройства хранения (network-attached storage, NAS) на ленту.

Определение использования накопителей библиотек при резервном копировании данных в библиотеки, подключенные к NAS

Благодаря гибкости конфигураций, допускаемых сервером IBM Spectrum Protect, накопители можно использовать для различных целей. Для операций NDMP файл-сервер NAS должен иметь доступ к накопителю. Сервер IBM Spectrum Protect также должен иметь доступ к тому же накопителю в зависимости от подключений и ограничений оборудования.

Об этой задаче

Все накопители назначаются серверу IBM Spectrum Protect. Однако один и тот же накопитель может быть задан как для традиционных операций IBM Spectrum Protect, так и для операций NDMP. На Рис. 1 показан один из возможных вариантов конфигурации. У сервера IBM Spectrum Protect есть доступ к накопителям 2 и 3, а у каждого файл-сервера NAS есть доступ к накопителям 1 и 2.
Рис. 1. Пример использования накопителей на сервере IBM Spectrum Protect



Чтобы создать конфигурацию, показанную на Рис. 1, выполните следующие шаги:

Процедура

1. Назначьте все три накопителя серверу IBM Spectrum Protect.
2. Задайте пути от сервера IBM Spectrum Protect к накопителям 2 и 3. Поскольку накопитель 1 не используется сервером, указывать путь не нужно.
3. Задайте каждый файл-сервер NAS как отдельный узел перемещения данных.
4. Задайте пути от каждого узла перемещения данных к накопителям 1 и 2.

Результаты

Чтобы использовать внутренние операции перемещения данных IBM Spectrum Protect, серверу IBM Spectrum Protect требуются два доступных пути к накопителям от одного узла перемещения данных NAS. Накопители могут располагаться в разных библиотеках и типы их могут быть разными (если они поддерживаются NDMP). Вы можете создавать копии для двух разных ленточных устройств. Например, исходным типом накопителя может быть накопитель DLT в одной библиотеке, а накопитель, на который производится копирование, может быть накопителем LTO в другой библиотеке.

Во время внутренних операций перемещения данных IBM Spectrum Protect сервер IBM Spectrum Protect находит узел перемещения данных NAS, которое поддерживает тот же формат, что используется для копируемых данные, и у которого есть две доступные точки монтирования и пути к накопителям. Если серверу IBM Spectrum Protect не удается найти такой узел, то запрошенная операция по перемещению данных не выполняется. Количество доступных точек монтирования и накопителей зависит от ограничений на монтирование в классах устройств пулов хранения, задействованных в операциях внутреннего перемещения данных.

Если функция внутреннего перемещения данных поддерживает многопроцессорную обработку, для каждого параллельного процесса внутреннего перемещения данных на сервере IBM Spectrum Protect необходимы две доступные точки монтирования и два накопителя. Для одновременного запуска двух процессов IBM Spectrum Protect необходимы минимум четыре доступных точки монтирования и четыре накопителя.

Дополнительные сведения смотрите в разделе Определение путей для операций NDMP.

Конфигурирование ленточной библиотеки для операций NDMP

Ленточную библиотеку можно сконфигурировать для резервного копирования сетевого устройства хранения (network-attached storage, NAS) на ленту.

Процедура

Чтобы настроить ленточные библиотеки для выполнение операций NDMP, выполните следующие действия:

1. Подключите библиотеку и накопители, которые будут использоваться для выполнения операций NDMP.
   a. Подключите библиотеку SCSI. Перед конфигурированием ленточной библиотеки SCSI для операций NDMP определите, к какому серверу, IBM Spectrum Protect или файл-серверу NAS, должно быть подключено устройство управления библиотекой. Смотрите раздел Ленточные библиотеки и накопители для операций NDMP. Подключите механизм управления ленточной библиотекой SCSI к серверу IBM Spectrum Protect или к файл-серверу NAS. Для получения инструкций обратитесь к документации производителя.

      Если библиотека подсоединена к IBM Spectrum Protect, установите соединение SCSI или Fibre Channel между сервером IBM Spectrum Protect и портом управления устройством библиотеки. Затем соедините файл-сервер NAS с накопителями.

      Если библиотека подсоединена к файл-серверу NAS, установите соединение SCSI или Fibre Channel между файл-сервером NAS и устройством и накопителями библиотеки.

   b. Подключите библиотеку ACSLS. Подключите библиотеку ACSLS к серверу IBM Spectrum Protect.
   c. Подключите библиотеку 349X. Подключите библиотеку 349X к серверу IBM Spectrum Protect.
2. Определите библиотеку для вашего устройства, введя команду DEFINE LIBRARY. Библиотека должна содержать устройства только одного типа, а не нескольких. Введите одну из следующих команд для определения библиотеки в зависимости от типа устройства, которое вы конфигурируете:

   Библиотека SCSI

   ```
   define library tsmlib libtype=scsi
   ```

   Библиотека ACSLS

   ```
   define library acslib libtype=acsls acsid=1
   ```

   Библиотека 349X

   ```
   define library tsmlib libtype=349x
   ```

3. Определите класс для вашего устройства NDMP, введя команду DEFINE DEVCLASS.
   Совет: Класс устройств, определяемый с типом устройств NAS, явно не связан с конкретным типом носителей, например с LTO. Однако рекомендуется определять отдельный класс устройств для разных типов носителей.
   В команде DEFINE DEVCLASS используйте следующие параметры и значения:
   - Задайте `DEVTYPE=NAS`.
   - Задайте `MOUNTRETENTION=0`. Это требуется для операций NDMP.
   - Укажите значение для параметра ESTCAPACITY.

   Например, чтобы определить класс устройств с именем NASCLASS для библиотеки с именем NASLIB с примерной емкостью носителей 40 ГБайт, введите следующую команду:

   ```
   define devclass nasclass devtype=nas library=naslib mountretention=0
    estcapacity=40g
   ```

4. Определите пул хранения для носителя NDMP, введя команду DEFINE STGPOOL. Когда NETAPPDUMP, CELERRADUMP или NDMPDUMP обозначены как тип пула хранения, управление пулами хранения, созданными при операциях NDMP, отличается от управления пулами хранения, содержащих носители для традиционных резервных копий IBM Spectrum Protect. Операции IBM Spectrum Protect используют пулы хранения, определенные с форматом данных

NATIVE или NONBLOCK. Если выбрать формат данных NETAPPDUMP, CELERRADUMP или NDMPDUMP, для выполнения операций NDMP понадобятся пулы хранения, формат данных которых совпадает с форматом данных файл-сервера NAS и выбранного метода резервного копирования. Рекомендуется поддерживать отдельные пулы хранения для данных от разных поставщиков NAS, хотя в обоих пулах формат данных - это NDMPDUMP. Например, чтобы определить пул хранения с именем NDMPPOOL для файл-сервера, не являющегося файл-сервером NetApp или Celerra, введите следующую команду:

```
define stgpool ndmppool nasclass maxscratch=10 dataformat=ndmpdump
```

Чтобы задать пул хранения с именем NASPOOL для файл-сервера NetApp, введите следующую команду:

```
define stgpool naspool nasclass maxscratch=10 dataformat=netappdump
```

Чтобы задать пул хранения с именем CELERRAPOOL для файл-сервера EMC Celerra, введите следующую команду:

```
define stgpool celerrapool nasclass maxscratch=10 dataformat=celerradump
```

Внимание: Убедитесь, что вы не используете случайно пулы хранения, определенные для операций NDMP, в традиционных операциях IBM Spectrum Protect. Особая осторожность необходима при присвоении пулу хранения имени, совпадающего со значением параметра DESTINATION команды DEFINE COPYGROUP. Если конечное расположение не является пулом хранения с соответствующим форматом данных, при резервном копировании может произойти ошибка.

5. Необязательно: Задайте пул, в котором будет храниться содержание (Table of Contents - TOC). Если вы собираетесь создавать содержание, необходимо также задать дисковый пул для его хранения. Необходимо задать политику, согласно которой сервер IBM Spectrum Protect будет сохранять содержание и резервную копию образа в разных пулах хранения. Содержание обрабатывается так же, как и любой другой объект в данном пуле хранения. Например, чтобы задать пул хранения с именем TOCPOOL для класса устройств DISK, введите следующую команду:

   ```
   define stgpool tocpool disk
   ```

   Затем задайте тома для пула хранения.

   Операционные системы AIXОперационные системы LinuxДополнительные сведения об определении томов смотрите в разделе Конфигурирование томов с произвольным доступом на дисковых устройствах (V7.1.1).

   Операционные системы WindowsДополнительные сведения об определении томов смотрите в разделе Конфигурирование томов с произвольным доступом на дисковых устройствах (V7.1.1).

   Операционные системы AIXОперационные системы LinuxДополнительную информацию о конфигурировании библиотек смотрите по адресу: Конфигурирование библиотек для использования сервером.

Ссылки, связанные с данной:
DEFINE DEVCLASS (Задать класс устройств)

Подключение устройств ленточных библиотек при использовании случае библиотек, подключенных к NAS

Если вы собираетесь создать резервную копию данных NAS в библиотеке, подключенной непосредственно к устройству NAS и используете ленточную библиотеку SCSI, вы должны решить, куда следует подключить библиотеку.

Об этой задаче

Необходимо определить, к какому из серверов подключать библиотечное устройство: к серверу IBM Spectrum Protect или файл-серверу NAS. Независимо от того, где подключено устройство библиотеки, для операций NDMP ленточные накопители должны всегда быть подключены к файл-серверу NAS.

При подключении SCSI-библиотек необходимо учитывать расстояние и имеющиеся подключения оборудования. Если библиотека не имеет отдельных портов для управления устройством библиотеки и доступа к накопителям, ее необходимо подключить к файл-серверу NAS, так как файл-сервер NAS должен иметь доступ к накопителям. Если же SCSI-библиотека имеет отдельные порты для управления устройством библиотеки и доступа к накопителям, ее устройство можно подключить либо к серверу IBM Spectrum Protect, либо к файл-серверу NAS. Если файл-сервер NAS и сервер IBM Spectrum Protect располагаются в разных местах, возможно, библиотеку, в зависимости от расстояния, необходимо будет подключить к файл-серверу NAS.

Независимо от того, какой тип библиотеки используется — SCSI, ACSLS, или 349X — есть возможность выделить библиотеку под операции NDMP либо использовать библиотеку для операций NDMP. Также можно использовать библиотеку для большинства традиционных операций IBM Spectrum Protect.

Табл. 1. Сводная информация о конфигурации для операций NDMP

Конфигурация	Расстояние между сервером IBM Spectrum Protect и библиотекой	Совместное использование библиотек	Совместное использование накопителей сервером IBM Spectrum Protect и файл-сервером NAS	Совместное использование накопителей файл-серверами NAS	Совместное использование накопителей агентом хранения и файл-сервером NAS
Конфигурация 1 (библиотека SCSI, подключенная к серверу IBM Spectrum Protect)	Ограничено подключением SCSI или FC	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Конфигурация 2 (библиотека SCSI, подключенная к файл-серверу NAS)	Ограничений нет	Не поддерживается	Поддерживается	Поддерживается	Не поддерживается
Конфигурация 3 (библиотека 349X)	Может ограничиваться соединением 349X	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Операционные системы AIX Операционные системы Windows Конфигурация 4 (библиотека ACSLS)	Операционные системы AIX Операционные системы Windows Может ограничиваться соединением ACSLS	Операционные системы AIX Операционные системы Windows Поддерживается	Операционные системы AIX Операционные системы Windows Поддерживается	Операционные системы AIX Операционные системы Windows Поддерживается	Операционные системы AIX Операционные системы Windows Поддерживается

- Конфигурация 1: Библиотека SCSI, подключенная к серверу IBM Spectrum Protect
  В этой конфигурации библиотека лент должна иметь отдельные порты для управления устройством библиотеки и доступа к накопителям. Кроме того, библиотека должна поддерживать возможность подключения по обноволоконным каналами или подключения SCSI к серверу IBM Spectrum Protect и файл-серверу NAS.
- Конфигурация 2: Библиотека SCSI, подключенная к файл-серверу NAS
  В этой конфигурации устройство библиотеки и накопители должны быть физически подключены непосредственно к файл-серверу NAS. Пути должны быть определены от устройства перемещения данных к библиотеке и накопителям. Физического соединения между библиотекой SCSI и сервером IBM Spectrum Protect не требуется.
- Конфигурация 3: Библиотека 349x, подключенная к серверу IBM Spectrum Protect
  В этой конфигурации библиотека ленточных носителей подключается к системе, как для традиционных операций.
- Конфигурация 4: Библиотека ACSLS, подключенная к серверу IBM Spectrum Protect.
  В этой конфигурации библиотека ленточных носителей подключается к системе, как для традиционных операций IBM Spectrum Protect.

Конфигурация 1: Библиотека SCSI, подключенная к серверу IBM Spectrum Protect

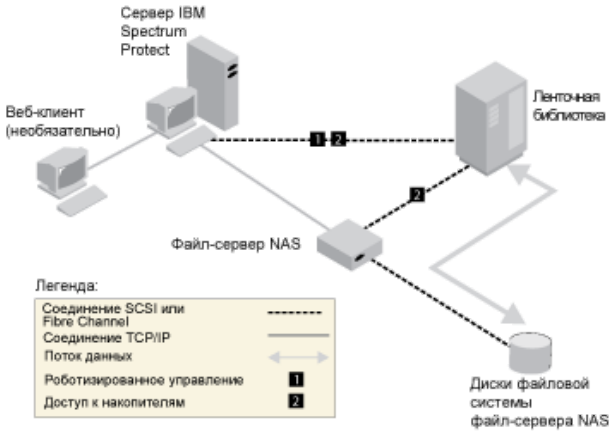
В этой конфигурации библиотека лент должна иметь отдельные порты для управления устройством библиотеки и доступа к накопителям. Кроме того, библиотека должна поддерживать возможность подключения по обноволоконным каналами или подключения SCSI к серверу IBM Spectrum Protect и файл-серверу NAS.

В этой конфигурации сервер IBM Spectrum Protect управляет SCSI-библиотекой через прямое физическое соединение с портом управления устройством библиотеки. Для операций NDMP накопители в библиотеке подключаются непосредственно к файл-серверу NAS, при этом необходимо указать путь от устройства перемещения данных NAS к каждому используемому накопителю. Файл-сервер NAS передает данные на ленточный накопитель по запросу сервера

IBM Spectrum Protect. Чтобы накопители можно было использовать для операций сервера IBM Spectrum Protect, подключите сервер IBM Spectrum Protect к ленточным накопителям и определите пути к ним от сервера.

Эта конфигурация также поддерживает доступ агента хранения IBM Spectrum Protect к накопителям для операций в режиме без локальной сети, а сервер IBM Spectrum Protect может выступать менеджером библиотеки.

Рис. 1. Конфигурация 1: библиотека SCSI подключена к серверу IBM Spectrum Protect

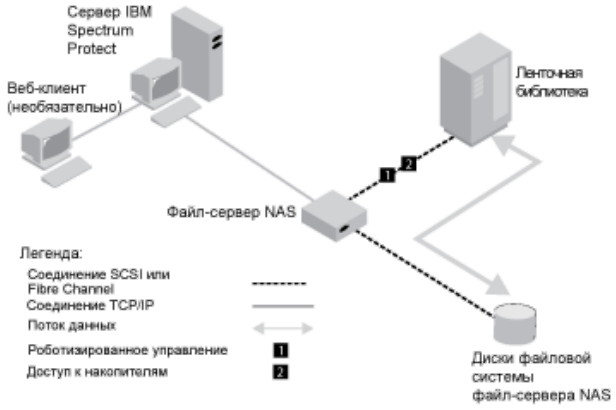


Конфигурация 2: Библиотека SCSI, подключенная к файл-серверу NAS

В этой конфигурации устройство библиотеки и накопители должны быть физически подключены непосредственно к файл-серверу NAS. Пути должны быть определены от устройства перемещения данных к библиотеке и накопителям. Физического соединения между библиотекой SCSI и сервером IBM Spectrum Protect не требуется.

Сервер IBM Spectrum Protect управляет механизмом библиотеки, передавая по сети команды библиотеки файл-серверу NAS. Файл-сервер NAS передает команды библиотеке лент. Любые ответы, произведенные библиотекой, отправляются в файловый сервер NAS и пасуются назад по сети к IBM Spectrum Protect сервер Этак конфигурация поддерживает сервер IBM Spectrum Protect и файл-сервер NAS, физически удаленные друг от друга. Например, IBM Spectrum Protect в то время как файловый сервер NAS и ленточная библиотека находятся в другом городе, сервер находится в одном городе.

Рис. 1. Конфигурация 2: библиотека SCSI подключена к файл-серверу NAS



Конфигурация 3: Библиотека 349x, подключенная к серверу IBM Spectrum Protect

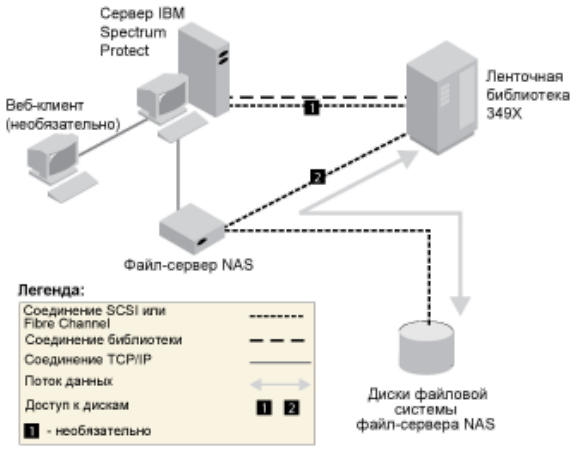
В этой конфигурации библиотека ленточных носителей подключается к системе, как для традиционных операций.

В этой конфигурации ленточной библиотекой 349X управляет сервер IBM Spectrum Protect. Сервер IBM Spectrum Protect осуществляет управление библиотекой путем передачи запроса менеджеру библиотеки 349X через TCP/IP.

Для завершения NAS (сетевое хранилище данных) копируют или восстанавливают операции, файловый сервер NAS должен быть в состоянии получить доступ к одному или более лентопротяжным устройствам в 349X библиотека. Любые из используемых для операций NAS ленточных накопителей должны быть физически подключены к файл-серверу NAS, при этом необходимо определить пути от устройства перемещения данных NAS к накопителям. Файл-сервер NAS передает данные на ленточный накопитель по запросу сервера IBM Spectrum Protect. Для подключения накопителя к системе сервера следуйте инструкциям производителя.

Этак конфигурация поддерживает физически удаленные сервер IBM Spectrum Protect и файл-сервер NAS. Например, сервер IBM Spectrum Protect может находиться в одном городе, а файл-сервер nAS и библиотека лент - в другом.

Рис. 1. Конфигурация 3: Библиотека 349x, подключенная к серверу IBM Spectrum Protect



Информация, связанная с данной:
Подключение устройств для сервера

Конфигурация 4: Библиотека ACSLS, подключенная к серверу IBM Spectrum Protect.

В этой конфигурации библиотека ленточных носителей подключается к системе, как для традиционных операций IBM Spectrum Protect.

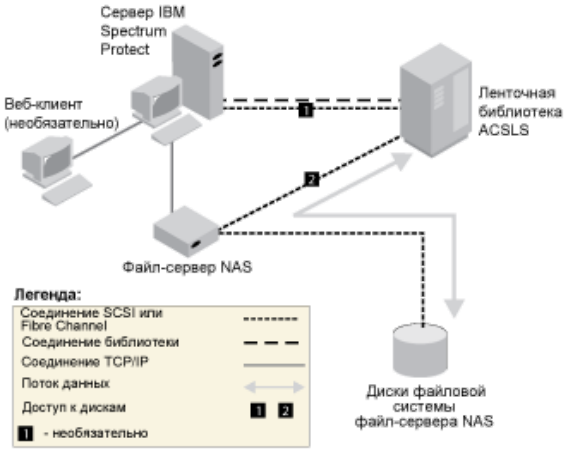
Ленточной библиотекой ACSLS (Automated Cartridge System Library Software) управляет сервер IBM Spectrum Protect. Сервер IBM Spectrum Protect осуществляет управление библиотекой путем передачи запроса серверу библиотеки ACSLS по TCP/IP. Библиотека ACSLS поддерживает совместное использование и операции в режиме без локальной сети. Операционные системы WindowsОграничение: Чтобы воспользоваться функциями ACSLS, надо установить программу StorageTek Library Attach. Дополнительные сведения смотрите в разделе: Библиотеки под управлением ACSLS (V7.1.1).

Чтобы осуществлять операции резервного копирования и восстановления NAS (Network Attached Storage), файл-сервер NAS должен иметь доступ к одному или нескольким накопителям в библиотеке ACSLS. Используемые для операций NAS ленточные накопители должны быть физически подключены к файл-серверу NAS, при этом необходимо указать пути от устройства перемещения данных NAS к накопителям. Файл-сервер NAS передает данные на ленточный накопитель по запросу сервера IBM Spectrum Protect. Для подключения накопителя к системе сервера следуйте инструкциям производителя.

Этак конфигурация поддерживает сервер IBM Spectrum Protect и файл-сервер NAS, физически удаленные друг от друга. Например, сервер IBM Spectrum Protect может находиться в одном городе, а файл-сервер nAS и библиотека лент - в другом.

Чтобы накопители можно было использовать для операций сервера IBM Spectrum Protect, подключите сервер IBM Spectrum Protect к ленточным накопителям и определите пути к ним от сервера IBM Spectrum Protect.

Рис. 1. Конфигурация 4: библиотека ACSLS подключена к серверу IBM Spectrum Protect.



Информация, связанная с данной:

Подключение устройств для сервера

Регистрация узлов NAS на сервере IBM Spectrum Protect

Зарегистрируйте файл-сервер NAS в качестве узла IBM Spectrum Protect, указав TYPE=NAS. Это имя узла используется для отслеживания резервных копий образов для файл-сервера NAS.

Процедура

Чтобы зарегистрировать файл-сервер NAS в качестве узла с именем NASNODE1 и паролем NASPWD1 в домене политики с именем NASDOMAIN, введите команду следующего вида:

```
register node nasnode1 naspwd1 domain=nasdomain type=nas
```

Если используется клиентский набор параметров, его необходимо указать при регистрации узла.
Регистрацию узла можно проверить с помощью следующей команды:

```
query node type=nas
```

Напоминание: Необходимо указать TYPE=NAS, чтобы на экране появились только узлы NAS.

Как задать узел перемещения данных для файл-сервера NAS

Задайте узел перемещения данных для каждого файл-сервера NAS, использующего операции NDMP в вашей среде. Имя узла перемещения данных должно совпадать с именем узла, указанного при регистрации узла NAS на сервере IBM Spectrum Protect.

Об этой задаче

Определение узла перемещения данных NAS содержит сетевой адрес, авторизацию и форматы данных, необходимые для операций NDMP. Узел перемещения данных разрешает связь и обеспечивает полномочия для операций NDMP между сервером IBM Spectrum Protect и файл-сервером NAS.

Процедура

Чтобы задать функцию перемещения данных, используйте команду DEFINE DATAMOVER.

Пример

Например, задайте функцию перемещения данных со следующими параметрами:

- Узел NAS называется NASNODE1.
- Адресом высокого уровня является IP-адрес файл-сервера NAS — либо числовой адрес, либо имя хоста.

- Низкоуровневым адресом является IP-порт для сеансов NDMP с файл-сервером NAS. По умолчанию используется номер порта 10000.
- ID пользователя - это заданный для файл-сервера NAS ID, которому разрешено устанавливать сеанс NDMP с файл-сервером NAS. В данном примере ID пользователя - это ID администратора для файл-сервера NetApp.
- Значение параметра password - действующий пароль для аутентификации сеанса NDMP на файл-сервере NAS.
- Формат данных — NETAPPDUMP. Этот формат данных используется файл-сервером NetApp для операций резервного копирования на ленту. Формат данных должен совпадать с форматом данных целевого пула хранения.

Введите команду

```
define datamover nasnode1 type=nas hladdress=netapp2 lladdress=10000 userid=root
password=admin dataformat=netappdump
```

Ссылки, связанные с данной:
DEFINE DATAMOVER (Задать средство перемещения данных)

Определение путей для операций NDMP

Для операций NDMP надо создать пути к накопителям и библиотекам.

- Определение путей к накопителям для операций NDMP
  Способ, выбираемый для создания путей к накопителям, зависит от того, обращается ли к этим накопителям и файл-сервер NAS, и сервер IBM Spectrum Protect или только файл-сервер NAS.
- Определение путей к библиотекам для операций NDMP
  Укажите путь к библиотеке SCSI от сервера IBM Spectrum Protect либо от файл-сервера NAS (network attached storage).

Определение путей к накопителям для операций NDMP

Способ, выбираемый для создания путей к накопителям, зависит от того, обращается ли к этим накопителям и файл-сервер NAS, и сервер IBM Spectrum Protect или только файл-сервер NAS.

- Как задать пути для накопителей, подключенных к файл-серверу NAS и серверу IBM Spectrum Protect
  Если доступ к ленточному накопителю должен получать файл-сервер NAS (Network-Attached Storage) и сервер IBM Spectrum Protect, нужно создать два пути. Один путь существует между ленточным накопителем и файл-сервером NAS. Другой путь существует между ленточным накопителем и сервером IBM Spectrum Protect.
- Определение путей для накопителей, подключенных только к файл-серверам NAS
  Если доступ к ленточному накопителю должен получать только файл-сервер NAS, но не сервер IBM Spectrum Protect, требуется только один путь: между ленточным накопителем и файл-сервером NAS.
- Получение имен устройств, подключенных к файл-серверам NAS
  Для путей от устройства перемещения данных NAS значение параметра DEVICE в команде DEFINE PATH - это имя, по которому файл-сервер NAS идентифицирует библиотеку или накопитель.

Как задать пути для накопителей, подключенных к файл-серверу NAS и серверу IBM Spectrum Protect

Если доступ к ленточному накопителю должен получать файл-сервер NAS (Network-Attached Storage) и сервер IBM Spectrum Protect, нужно создать два пути. Один путь существует между ленточным накопителем и файл-сервером NAS. Другой путь существует между ленточным накопителем и сервером IBM Spectrum Protect.

Процедура

Сделайте следующее:

1. Если накопитель не определен для сервера IBM Spectrum Protect, создайте определение этого накопителя. Например, чтобы определить накопитель NASDRIVE1 для библиотеки NASLIB, введите следующую команду:

   ```
   define drive naslib nasdrive1 element=autodetect
   ```

   Напоминание: Если накопитель подключен к серверу IBM Spectrum Protect, адрес элемента определяется автоматически.

2. Отобразите имя накопителя NAS на соответствующее определение накопителя на сервере IBM Spectrum Protect:
   - На сервере IBM Spectrum Protect введите команду QUERY DRIVE FORMAT=DETAILED, чтобы получить имя WWN и серийный номер для накопителя, который будет соединен с файл-сервером NAS.
   - Для устройства NAS получите имя ленточного устройства, серийный номер и WWN для накопителя.

   Если WWN или серийный номер совпадает, накопитель на файл-сервере NAS будет тем же накопителем, что и на на сервере IBM Spectrum Protect.
3. Используя имя накопителя, определите путь к накопителю от файл-сервера NAS и путь к этому накопителю от сервера IBM Spectrum Protect.
   - Например, чтобы определить путь между ленточным накопителем с именем устройства rst01 и файл-сервером NetApp, введите следующую команду:

     ```
     define path nasnode1 nasdrive1 srctype=datamover desttype=drive
       library=naslib device=rst01
     ```

   - Чтобы определить путь между ленточным накопителем и сервером IBM Spectrum Protect, введите следующую команду:

      Операционные системы AIX

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=/dev/rmt0
     ```

      Операционные системы Linux

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=/dev/tsmscsi/mt0
     ```

      Операционные системы Windows

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=mt3.0.0.2
     ```

Определение путей для накопителей, подключенных только к файл-серверам NAS

Если доступ к ленточному накопителю должен получать только файл-сервер NAS, но не сервер IBM Spectrum Protect, требуется только один путь: между ленточным накопителем и файл-сервером NAS.

Процедура

Сделайте следующее:

1. Получите адреса элементов SCSI, всемирное имя (WWN) и серийные номера для накопителя, соединяемого с файл-сервером NAS.
   Ограничение: Если накопитель SCSI соединен только с файл-сервером NAS, адрес элемента автоматически не определяется. Если для библиотеки используется несколько накопителей, для каждого из них нужно указать адрес элемента.
   Чтобы получить адрес элемента SCSI, зайдите на следующие сайты поддержки устройств:
   -  Операционные системы AIX  Операционные системы WindowsПоддерживаемые устройства для AIX и Windows
   -  Операционные системы LinuxПоддерживаемые устройства для Linux

   Нумерацию элементов и назначенные устройствам WWN можно также получить у изготовителей устройств ленточных библиотек.
2. Создайте определения накопителей, указав адреса элементов, идентифицированные на предыдущем шаге. Адрес элемента задается в параметре ELEMENT команды DEFINE DRIVE. Например, чтобы определить накопитель NASDRIVE1 с адресом элемента 82 для библиотеки NASLIB, введите следующую команду:

   ```
   define drive naslib nasdrive1 element=82
   ```

   Внимание: В случае накопителя, подключенного только к файл-серверу NAS, задавать ASNEEDED в качестве значения для параметра CLEANFREQUENCY в команде DEFINE DRIVE не нужно.
3. Получите имя устройства, серийный номер и WWN для накопителя для устройства NAS.
4. С помощью информации, полученной на шаге 1 и 3, отобразите имя устройства NAS на адрес элемента в определении накопителя на сервере IBM Spectrum Protect.

5. Определите путь между ленточным накопителем и файл-сервером NAS. Например, чтобы определить путь между файл-сервером NetApp и ленточным накопителем с именем устройства rst01, введите следующую команду:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive
 library=naslib device=rst01
```

Получение имен устройств, подключенных к файл-серверам NAS

Для путей от устройства перемещения данных NAS значение параметра DEVICE в команде DEFINE PATH - это имя, по которому файл-сервер NAS идентифицирует библиотеку или накопитель.

Об этой задаче

Эти имена устройств (их называют также *специальные файловые имена*) можно получить, запросив файл-сервер NAS. Чтобы узнать, как получить имена устройств, подключенных к файл-серверу NAS, смотрите документацию по файл-серверу.

Процедура

- Чтобы получить имена устройств для ленточных библиотек в NetApp Release ONTAP 10.0 GX или новее (с файл-сервера), соединитесь с файл-сервером при помощи telnet и введите команду SYSTEM HARDWARE TAPE LIBRARY SHOW. Чтобы получить имена устройств для ленточных накопителей в NetApp Release ONTAP 10.0 GX или новее (с файл-сервера), соединитесь с файл-сервером при помощи telnet и введите команду SYSTEM HARDWARE TAPE DRIVE SHOW. Подробную информацию об этих командах смотрите в документации по файл-серверу NetApp ONTAP GX.
- Если вы используете более ранний выпуск, чем NetApp Release ONTAP 10.0 GX, продолжайте использовать команду SYSCONFIG. Например, чтобы узнать имена устройств для ленточных библиотек, соединитесь с файл-сервером при помощи Telnet и введите следующую команду:

  ```
  sysconfig -m
  ```

  Чтобы узнать имена устройств для ленточных накопителей, введите следующую команду:

  ```
  sysconfig -t
  ```

- Для накопителей, подключенных по оптоволоконным каналам, и для устройств перемещения данных Celerra выполните следующие действия:
  1. Войдите в систему управляющей рабочей станции EMC Celerra, используя ID администратора. Введите следующую команду:

     ```
     server_devconfig server_1 -l -s -n
     ```

     Совет: Опция -l для этой команды возвращает только информацию об устройстве, которая была сохранена в базе данных устройства перемещения данных. Эта опция команды не выводит изменения, внесенные в конфигурацию устройства после последнего обновления базы данных устройства перемещения данных. Подробности о получении новейшей конфигурации для устройства перемещения данных смотрите в документации по EMC Celerra.
     Вывод команды server_devconfig содержит имена устройств, подключенных к устройству перемещения данных. Имена устройств выводятся в столбце *addr*, например:

     ```
     server_1:
     Scsi Device Table
     name        addr      type   info
     tape1       c64t0l0   tape   IBM ULT3580-TD2 53Y2
     ttape1      c96t0l0   tape   IBM ULT3580-TD2 53Y2
     ```

  2. Отобразите имя устройства Celerra на всемирное имя устройства (device worldwide name, WWN):
     a. Чтобы получить WWN, войдите в систему управляющей рабочей станции EMC Celerra и введите следующую команду. Не забудьте ввести точку (.) в качестве первого символа этой команды.

        ```
        .server_config server_# -v "fcp bind show"
        ```

        Вывод этой команды содержит WWN, например:

        ```
        Chain 0064: WWN 500507630f418e29 HBA 2 N_PORT Bound
        Chain 0096: WWN 500507630f418e18 HBA 2 N_PORT Bound
        ```

Совет: Команда .server_config - недокументированная команда EMC Celerra. За дополнительной информацией о ее использовании обращайтесь в EMC.

b. Номер цепочки служит для идентификации ленточного устройства, указанного в выводе команды server_devconfig, и с тем же самым WWN, например:

Имя ленточного устройства	Номер цепочки	WWN
c64t0l0	0064	500507630f418e29
c96t0l0	0096	500507630f418e18

Команды Celerra для различных систем EMC Celerra и разных уровней операционной системы могут вести себя по-разному. Посмотрите подробности в документации EMC Celerra, либо обратитесь в EMC.

Определение путей к библиотекам для операций NDMP

Укажите путь к библиотеке SCSI от сервера IBM Spectrum Protect либо от файл-сервера NAS (network attached storage).

Процедура

1. Чтобы задать путь от сервера SERVER1 к библиотеке SCSI с именем TSMLIB, подключенной к IBM Spectrum Protect, введите, например, следующую команду:

   Операционные системы AIX

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/lb1
   ```

   Операционные системы Linux

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/tsmscsi/lb1
   ```

   Операционные системы Windows

   ```
   define path server1 tsmlib srctype=server desttype=library
          device=lb0.0.0.2
   ```

2. Чтобы задать путь от устройства перемещения данных NetApp NAS с именем NASNODE1 к библиотеке с именем NASLIB, подключенной к файл-серверу NAS, введите, например, следующую команду:

   ```
   define path nasnode1 naslib srctype=datamover desttype=library device=mc0
   ```

3. В случае библиотеки 349X, задайте путь к библиотеке от сервера IBM Spectrum Protect. Например, чтобы задать путь от сервера с именем SERVER1 к библиотеке 349X с именем TSMLIB, введите следующую команду:

   Операционные системы AIX

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/lmcp0
   ```

   Операционные системы Linux Операционные системы Windows

   ```
   define path server1 tsmlib srctype=server desttype=library
    device=library1
   ```

   Совет: The DEFINE PATH команда не требуется для библиотеки автоматизированного программного обеспечения системной библиотеки картриджей (ACSLS).

Планирование операций NDMP

Можно запланировать операции резервного копирования или восстановления для изображений, произведенных операциями NDMP. Используйте административные расписания, которые обрабатывают административные команды BACKUP NODE и RESTORE NODE.

Процедура

Создайте административное расписание при помощи команды DEFINE SCHEDULE. Например, чтобы создать административное расписание с именем NASSCHED для резервного копирования всех файловых систем узла NASNODE1, введите следующую команду:

```
define schedule nassched type=administrative cmd='backup node nasnode1' active=yes
starttime=20:00 period=1 perunits=days
```

Расписание активно и будет запускаться ежедневно в 20:00.
Ограничение: Команды BACKUP NODE и RESTORE NODE можно использовать только для узлов типа TYPE=NAS.
Задачи, связанные с данной:
Настройка расписания для ежедневных операций
Ссылки, связанные с данной:
BACKUP NODE (резервное копирование узла NAS)
RESTORE NODE (восстановление узла NAS)
DEFINE SCHEDULE (определение расписания выполнения административных команд)

Как задать виртуальные файловые пространства

Используйте определение виртуального файлового пространства для резервного копирования NAS на уровне каталогов. Для сокращения времени выполнения резервного копирования и восстановления больших файловых систем можно сопоставить путь к каталогу от файл-сервера NAS с именем виртуального файлового пространства на сервере IBM Spectrum Protect.

Процедура

Чтобы создать имя виртуального файлового пространства для пути к каталогу на устройстве NAS, введите команду DEFINE VIRTUALFSMAPPING:

```
define virtualfsmapping nas1 /mikesdir /vol/vol1 /mikes
```

Эта команда определяет имя виртуального файлового пространства /MIKESDIR на сервере, которое соответствует пути к каталогу /VOL/VOL1/MIKES на файл-сервере NAS, представленном узлом NAS1. Дополнительную информацию смотрите в разделе Резервное копирование и восстановление для операций NDMP.

Резервное копирование данных с использованием функции лента-на-ленту

При использовании функции NDMP для копирования с ленты на ленту для резервного копирования данных типом библиотеки может быть SCSI, 349X или ACSLS (automated cartridge system library software). Накопители могут использоваться совместно устройствами NAS и сервером IBM Spectrum Protect.

Об этой задаче

При использовании функции NDMP для копирования с ленты на ленту настройка конфигурации может влиять на производительность внутреннего перемещения данных в IBM Spectrum Protect.

Процедура

Чтобы задать одно устройство NAS с путями к четырем накопителям в библиотеке, введите команду MOVE DATA после завершения настройки конфигурации. Эта команда перемещает данные тома VOL1 в любые доступные тома того же пула хранения:

```
move data vol1
```

Перемещение данных с использованием функции копирования с ленты на ленту

Чтобы переместить данные с ленточного накопителя, основанного на более старой технологии, на ленточный накопитель, основанный на более новой технологии, используя операцию NDMP копирования с ленты на ленту, вы должны выполнить

стандартные шаги по настройке конфигурации, а также дополнительные шаги.

Об этой задаче

При использовании функции NDMP для копирования с ленты на ленту настройка конфигурации может влиять на производительность внутреннего перемещения данных в IBM Spectrum Protect.

Процедура

В дополнение к стандартным шагам по настройке конфигурации выполните следующие шаги:

1. Определите один накопитель в библиотеке lib1 со старой ленточной технологией:

   ```
   define drive lib1 drv1 element=1035
   ```

2. Определите один накопитель в библиотеке с новой ленточной технологией:

   ```
   define drive lib2 drv1 element=1036
   ```

3. Задайте пути с файл-сервера NAS на каждый накопитель:

   ```
   define path nas1 drv1 sourcetype=datamover desttype=drive library=lib1 device=rst11
   define path nas1 drv1 sourcetype=datamover desttype=drive library=lib2 device=rst21
   ```

4. Переместите данные из тома vol1 первичного пула хранения в тома другого первичного пула хранения, nasprimpool2:

   ```
   move data vol1 stgpool=nasprimpool2
   ```

Конфигурирование IBM Spectrum Protect для операций NDMP в кластеризованной среде NetApp

Вы можете производить резервное копирование данных из кластера NetApp на непосредственно подключенное ленточное устройство или на сервер IBM Spectrum Protect, который хранит данные в пуле хранения. Можно создать резервную копию всего кластера на одном узле IBM Spectrum Protect или частей кластера на нескольких узлах.

Прежде чем начать

Обзор функций NDMP в IBM Spectrum Protect и файл-серверов NetApp смотрите в техническом замечании 7046965. В этом техническом замечании также перечислены требования к системе.

Об этой задаче

Вы можете производить резервное копирование данных в кластеризованной среде NetApp на следующие носители хранения:

Ленточное устройство, непосредственно подключенное к файл-серверу NAS
: Вы можете производить резервное копирование данных на ленточное устройство, непосредственно подключенное к файл-серверу NAS. Это предпочтительный метод. Как правило, быстрее создать резервную копию данных на непосредственно подключенном ленточном устройстве, чем производить резервное копирование данных в пул хранения IBM Spectrum Protect, используя сетевое соединение.

Пул хранения в локальной иерархии IBM Spectrum Protect
: Вы можете производить резервное копирование данных на сервер IBM Spectrum Protect, который хранит данные в пуле хранения типа DISK, FILE или в ленточном пуле хранения. Преимуществом хранения данных в пуле хранения является возможность реплицировать данные для дополнительной защиты данных. Можно использовать существующие пулы хранения или создать пулы хранения. У вас должно быть сетевое соединение между файл-сервером NAS и сервером IBM Spectrum Protect. У сетевого соединения должна быть достаточная полоса пропускания для передачи данных резервных копий NAS.
  Совет: Этот тип резервного копирования иногда называют резервным копированием с файл-сервера на сервер.

Можно использовать один из следующих методов резервного копирования:

Полное резервное копирование кластера

При использовании этого метода владельцем данных резервной копии всего кластера является один узел IBM Spectrum Protect. Даже если вы перемещаете тома в пределах кластера, операция полного резервного копирования продолжится, и переконфигурировать операции резервного копирования не потребуется. Это предпочтительный метод.

Частичное резервное копирование кластера

При применении этого метода вы задаете виртуальную машину хранения (storage virtual machine, SVM) NetApp, которая определяет область операции резервного копирования. SVM - это виртуальный сервер, обеспечивающий доступ к части кластера. Вы можете указать, что каждая SVM в кластере производит резервное копирование данных на отдельный узел IBM Spectrum Protect. При таком методе требуется выполнить больше задач по конфигурированию, чем при методе полного резервного копирования кластера, и потребуется сетевое соединение для передачи данных с SVM на узел IBM Spectrum Protect.

Ограничение: Использовать этот метод для резервного копирования данных на ленточное устройство нельзя, так как у SVM нет непосредственного доступа к ленточным устройствам.

Процедура

1. Выберите носитель хранения на основе следующих вопросов:

Вопрос	Носитель хранения
Если исходить из ваших бизнес-требований, нужно ли производить резервное копирование данных на локальное ленточное устройство?	Если да, то используйте непосредственно подключенное ленточное устройство. Если нет, то используйте либо непосредственно подключенное ленточное устройство, либо локальный пул хранения IBM Spectrum Protect.
Требуются ли вашей организации высокоскоростные операции резервного копирования?	Если да, то используйте непосредственно подключенное ленточное устройство. Если нет, то используйте либо непосредственно подключенное ленточное устройство, либо локальный пул хранения IBM Spectrum Protect.
Располагает ли ваша организация достаточной сетевой полосой пропускания для данных резервных копий NAS?	Если да, используйте либо непосредственно подключенное ленточное устройство, либо локальный пул хранения IBM Spectrum Protect. Если нет, используйте непосредственно подключенное ленточное устройство.
Расширяет ли ваша организация защиту данных, используя репликацию?	Если да, используйте локальный пул хранения IBM Spectrum Protect. Если нет, то используйте либо непосредственно подключенное ленточное устройство, либо локальный пул хранения IBM Spectrum Protect.
Ваши файл-серверы NAS в удаленном расположении не имеют доступа к непосредственно подключенным ленточным библиотекам?	Если да, используйте локальный пул хранения IBM Spectrum Protect. Если нет, то используйте либо непосредственно подключенное ленточное устройство, либо локальный пул хранения IBM Spectrum Protect.

2. Выберите метод резервного копирования на основе следующих вопросов:

Вопрос	Метод резервного копирования
Если исходить из ваших бизнес-требований, нужно ли производить резервное копирование данных на непосредственно подключенное ленточное устройство?	Если да, используйте метод полного резервного копирования. Если нет, используйте метод либо полного, либо частичного резервного копирования.
Есть ли у вашей системы достаточная сетевая полоса пропускания для резервного копирования нескольких SVM, так чтобы это не влияло на производительность сети?	Если да, используйте метод либо полного, либо частичного резервного копирования. Если нет, используйте метод полного резервного копирования. Метод частичного резервного копирования может отрицательно повлиять на производительность системы.

Вопрос	Метод резервного копирования
Распределены ли SVM по нескольким организациям? Так, есть ли какие-либо SVM, управляемые третьими сторонами, например, провайдерами платформ облака?	Если да, используйте метод частичного резервного копирования, так как владельцы SVM смогут управлять операциями резервного копирования для отдельных SVM. Если владелец SVM также является владельцем сервера IBM Spectrum Protect, владелец может задать операции резервного копирования с SVM на узел сервера. Это даст владельцу возможность управлять процессом от начала и до конца. Если нет, используйте метод либо полного, либо частичного резервного копирования.

3. Сконфигурируйте системную среду на основе носителя хранения и выбранного вами метода резервного копирования. Выполните инструкции для выбранного вами метода:
    - Конфигурирование полного резервного копирования кластера на непосредственно подключенные ленточные устройства
    - Конфигурирование полного резервного копирования кластера на сервер IBM Spectrum Protect
    - Конфигурирование частичного резервного копирования кластера на сервер IBM Spectrum Protect

   Совет: Если вы сконфигурировали IBM Spectrum Protect для резервного копирования кластеров NetApp с использованием NDMP в области узлов, рассмотрите возможность переконфигурирования IBM Spectrum Protect для использования NDMP Cluster Aware Backup (CAB). Это позволит оптимизировать операции резервного копирования для кластеров NetApp. Следуйте инструкциям в разделе Переконфигурирование IBM Spectrum Protect для оптимизации кластеризованного резервного копирования.

- Конфигурирование полного резервного копирования кластера на непосредственно подключенные ленточные устройства
  Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования всех томов в кластере NetApp на непосредственно подключенное ленточное устройство.
- Конфигурирование полного резервного копирования кластера на сервер IBM Spectrum Protect
  Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования всех томов в кластере NetApp на сервер IBM Spectrum Protect, который хранит данные в пуле хранения. Даже если вы перемещаете тома в пределах кластера, резервное копирование продолжается, и переконфигурирование не требуется.
- Конфигурирование частичного резервного копирования кластера на сервер IBM Spectrum Protect
  Вы можете сконфигурировать IBM Spectrum Protect для выполнения частичного резервного копирования кластера NetApp. Этот метод полезен, если владельцами данных в кластере являются несколько организаций. Каждая организация может управлять операциями резервного копирования своих данных.
- Переконфигурирование IBM Spectrum Protect для оптимизации кластеризованного резервного копирования
  Если вы сконфигурировали IBM Spectrum Protect для резервного копирования кластеров NetApp с использованием NDMP в области узлов, вы можете переконфигурировать IBM Spectrum Protect для использования NDMP Cluster Aware Backup (CAB). Это позволит оптимизировать операции резервного копирования для кластеров NetApp.

Конфигурирование полного резервного копирования кластера на непосредственно подключенные ленточные устройства

Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования всех томов в кластере NetApp на непосредственно подключенное ленточное устройство.

Прежде чем начать

Обзор функций NDMP в IBM Spectrum Protect и файл-серверов NetApp смотрите в техническом замечании 7046965. В этом техническом замечании также перечислены требования к системе.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система будет установлена на ваш файл-сервер NetApp, используйте следующую процедуру. После конфигурирования файл-сервера NetApp для работы с IBM Spectrum Protect вы сможете использовать расширение NetApp Cluster Aware Backup (CAB) для резервного копирования всех томов.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система не будет установлена на ваш файл-сервер NetApp, то надо создать резервную копию данных, для чего надо выполнить инструкции в разделе Конфигурирование IBM Spectrum Protect для операций NDMP в некластеризованной среде.

Об этой задаче

Предпочтительный метод - резервное копирование всего кластера с использованием узла и средства перемещения данных, которые связаны с сетью в масштабах кластера. Это позволит вам убедиться, что владельцем данных резервных копий является один узел IBM Spectrum Protect. Даже если вы перемещаете тома в пределах кластера, резервное копирование продолжается, и переконфигурирование не требуется.

Процедура

Чтобы сконфигурировать операции полного резервного копирования кластера на непосредственно подключенное ленточное устройство, выполните следующие шаги:

1. Убедитесь, что у вас установлен продукт IBM Spectrum Protect Extended Edition и что лицензия зарегистрирована. Если лицензия не зарегистрирована, введите следующую команду IBM Spectrum Protect:

   ```
   register license file=tsmee.lic
   ```

2. Получите полномочия администратора кластера для файл-сервера NetApp. Этот шаг необходим для получения доступа к консоли кластера.
3. На файл-сервере NetApp разрешите использовать NDMP, выполнив инструкции в публикации *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Сделайте следующее:
   a. Включите операции резервного копирования NDMP в области SVM на уровне кластера. Это позволит отключить операции резервного копирования NDMP в области узла на файл-сервере NAS. Убедитесь, что для опции node-scoped-ndmp на файл-сервере NAS задано значение OFF.
   b. Создайте резервный ID пользователя для операций NDMP.
   c. Сконфигурируйте сетевой интерфейс для управления соединениями NDMP на уровне кластера.
4. Зарегистрируйте узел IBM Spectrum Protect, который будет владеть всеми данными резервного копирования для кластера. На сервере IBM Spectrum Protect введите команду REGISTER NODE:

   ```
   register node имя_узла пароль
   domain=домен_nas type=nas
   ```

   где *имя_узла* - это имя узла, *пароль* - это пароль узла, а *домен_nas* - это домен узла. Назначьте узел в домен, в котором есть политика для резервного копирования данных в соответствующий пул хранения.
5. Определите IP-адрес интерфейса управления кластером NetApp на файл-сервере NAS. Интерфейс предоставляет доступ ко всему кластеру. На файл-сервере NAS введите следующую команду операционной системы Data ONTAP:

   ```
   network interface show -role cluster-mgmt
   ```

   IP-адрес, показаный в выходных результатах команды - это обязательное значение, если вы задали параметр HLADDRESS на шаге 6.
6. Задайте узел перемещения данных для узла IBM Spectrum Protect, который станет владельцем резервной копии данных. На сервере IBM Spectrum Protect введите команду DEFINE DATAMOVER в одной строке:

   ```
   define
   datamover имя_средства_перемещения_данных type=nascluster
   hladdress=интерфейс_управления_кластером lladdress=порт
   USER=имя_пользователя password=пароль dataformat=netappdump
   ```

   где *интерфейс_управления_кластером* - это значение, которое вы получили на шаге 5, а *имя_средства_перемещения_данных* - это имя узла, зарегистрированное на шаге 4. Сведения о задании других параметров смотрите в разделе DEFINE DATAMOVER (Задать средство перемещения данных).
   Совет: После того как вы зададите средство перемещения данных, дополнительные средства перемещения данных будут автоматически заданы для каждого узла в кластере. Имя каждого средства перемещения данных соответствует имени физического узла в кластере. Вы будете использовать эти средства перемещения данных, когда будете задавать пути к ленточным накопителям в шаге 3 из Конфигурирование ленточных устройств для полного резервного копирования кластера.

Дальнейшие действия

Чтобы сконфигурировать ленточное устройство для полного резервного копирования кластера, следуйте инструкциям в разделе Конфигурирование ленточных устройств для полного резервного копирования кластера.

- Конфигурирование ленточных устройств для полного резервного копирования кластера
  Если вы собираетесь создавать резервные копии всех томов в кластере NetApp на непосредственно подключенном ленточном устройстве, вы должны сконфигурировать ленточное устройство.

Ссылки, связанные с данной:

Конфигурирование полного резервного копирования кластера на сервер IBM Spectrum Protect

Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования всех томов в кластере NetApp на сервер IBM Spectrum Protect, который хранит данные в пуле хранения. Даже если вы перемещаете тома в пределах кластера, резервное копирование продолжается, и переконфигурирование не требуется.

Прежде чем начать

Обзор функций NDMP в IBM Spectrum Protect и файл-серверов NetApp смотрите в техническом замечании 7046965. В этом техническом замечании также перечислены требования к системе.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система будет установлена на ваш файл-сервер NetApp, используйте следующую процедуру. После конфигурирования файл-сервера NetApp для работы с IBM Spectrum Protect вы сможете использовать расширение NetApp Cluster Aware Backup (CAB) для резервного копирования всех томов в кластере. Все резервные копии данных будут принадлежать одному узлу IBM Spectrum Protect.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система не будет установлена на ваш файл-сервер NetApp, то надо создать резервную копию данных, для чего надо выполнить инструкции в разделе Конфигурирование IBM Spectrum Protect для операций NDMP в некластеризованной среде.

Процедура

1. Убедитесь, что у вас установлен продукт IBM Spectrum Protect Extended Edition и что лицензия зарегистрирована. Если лицензия не зарегистрирована, введите следующую команду IBM Spectrum Protect:

   ```
   register license file=tsmee.lic
   ```

2. Получите полномочия администратора кластера для файл-сервера NetApp. Этот шаг необходим для получения доступа к консоли кластера.
3. Включите использование NDMP, выполнив инструкции в публикации *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Сделайте следующее:
   a. Включите NetApp SVM для управления операциями резервного копирования NDMP на уровне кластера.
   b. Создайте резервный ID пользователя для операций NDMP.
   c. Сконфигурируйте сетевой интерфейс для управления соединениями NDMP на уровне кластера.
4. Зарегистрируйте узел IBM Spectrum Protect, который будет владеть всеми данными резервного копирования для кластера. На сервере IBM Spectrum Protect введите команду REGISTER NODE:

   ```
   register node имя_узла пароль
   domain=домен_nas type=nas
   ```

   где *имя_узла* - это имя узла, *пароль* - это пароль узла, а *домен_nas* - это домен узла.
5. Определите цифровой IP-адрес, либо имя домена, используемые для доступа к файл-серверу NAS. Интерфейс предоставляет доступ ко всему кластеру. На файл-сервере NAS введите следующую команду операционной системы Data ONTAP:

   ```
   network interface show -role cluster-mgmt
   ```

   IP-адрес, показаный в выходных результатах - это обязательное значение, если вы задали параметр HLADDRESS на шаге 6.
6. Задайте средство перемещения данных для узла, введя команду DEFINE DATAMOVER и задав параметр `TYPE=NASCLUSTER`. На сервере IBM Spectrum Protect введите следующую команду в одной строке:

   ```
   define
   datamover имя_средства_перемещения_данных type=nascluster
   hladdress=интерфейс_управления_кластером lladdress=порт
   USER=имя_пользователя password=пароль dataformat=netappdump
   ```

   где *интерфейс_управления_кластером* - это значение, которое вы получили на шаге 5, а *имя_средства_перемещения_данных* - это имя узла, зарегистрированное на шаге 4. Сведения о задании других параметров смотрите в разделе DEFINE DATAMOVER (Задать средство перемещения данных).

7. Сконфигурируйте политику сервера IBM Spectrum Protect для управления резервными копиями образов NAS. Следуйте инструкциям в разделе Конфигурирование политики IBM Spectrum Protect для операций NDMP.
8. Обновите узел кластера, который вы зарегистрировали в шаге 4 для домена, сконфигурированного в шаге 7. На сервере IBM Spectrum Protect введите команду UPDATE NODE:

   ```
   update node имя_узла domain=имя_домена
   ```

9. Необязательно: Определите тома в кластере и запланируйте резервное копирование для томов:
   a. На файл-сервере NAS укажите тома в кластере, введя следующую команду Data ONTAP:

      ```
      volume show
      ```

   b. Запланируйте резервное копирование, выполнив инструкции в разделе Планирование операций NDMP.

Дальнейшие действия

Перечисленные ниже задачи являются необязательными:

- Чтобы проверить, производится ли резервное копирование томов в кластере NetApp, выполните следующее:
  1. В панели меню Центра операций выберите Клиенты.
  2. Дважды щелкните по клиенту устройства NAS и щелкните по Тома.
  3. Чтобы определить, когда было выполнено последнее полное резервное копирование тома, прочтите информацию в столбце Последнее полное. Чтобы определить, когда было выполнено последнее дифференциальное резервное копирование тома, прочтите информацию в столбце Последнее дифференциальное.
- Чтобы настроить пулы хранения копий для дополнительной защиты данных, сконфигурируйте функцию лента-лента для резервного копирования данных. Инструкции смотрите в разделе Резервное копирование данных с использованием функции лента-на-ленту.

Ссылки, связанные с данной:
REGISTER NODE (Зарегистрировать узел)

Конфигурирование частичного резервного копирования кластера на сервер IBM Spectrum Protect

Вы можете сконфигурировать IBM Spectrum Protect для выполнения частичного резервного копирования кластера NetApp. Этот метод полезен, если владельцами данных в кластере являются несколько организаций. Каждая организация может управлять операциями резервного копирования своих данных.

Прежде чем начать

Обзор функций NDMP в IBM Spectrum Protect и файл-серверов NetApp смотрите в техническом замечании 7046965. В этом техническом замечании также перечислены требования к системе.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система будет установлена на ваш файл-сервер NetApp, используйте следующую процедуру. После конфигурирования файл-сервера NetApp для работы с IBM Spectrum Protect вы сможете использовать расширение NetApp Cluster Aware Backup (CAB) для резервного копирования части кластера. При конфигурировании частичного резервного копирования кластера вы определяете область резервного копирования, задавая виртуальный сервер, NetApp Storage Virtual Machine (SVM). SVM обеспечивает доступ к части кластера.

Если версия NetApp Clustered Data ONTAP - 8.2 или новее, или 9.1 или новее, то операционная система не будет установлена на ваш файл-сервер NetApp, то надо создать резервную копию данных, для чего надо выполнить инструкции в разделе Конфигурирование IBM Spectrum Protect для операций NDMP в некластеризованной среде.

Процедура

1. Убедитесь, что у вас установлен продукт IBM Spectrum Protect Extended Edition и что лицензия зарегистрирована. Если лицензия не зарегистрирована, введите следующую команду IBM Spectrum Protect:

   ```
   register license file=tsmee.lic
   ```

2. Получите полномочия администратора кластера для файл-сервера NetApp. Этот шаг необходим для получения доступа к консоли кластера.
3. На файл-сервере NetApp разрешите использовать NDMP, выполнив инструкции в публикации *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Сделайте следующее:
    a. Включите NetApp SVM для управления операциями резервного копирования NDMP.
    b. Создайте резервный ID пользователя для операций NDMP.
    c. Сконфигурируйте сетевой интерфейс для управления соединениями NDMP на уровне SVM.
4. Зарегистрируйте узел IBM Spectrum Protect, который будет владеть резервными копиями данных. На сервере IBM Spectrum Protect введите команду REGISTER NODE:

    ```
    register node имя_узла пароль
    domain=домен_nas type=nas
    ```

    где *имя_узла* - это имя узла, *пароль* - это пароль узла, а *домен_nas* - это домен узла.
5. Определите цифровой IP-адрес либо имя домена интерфейса кластера, используемого SVM. Чтобы определить значение, введите на файл-сервере NAS следующую команду операционной системы ONTAP:

    ```
    network interface show -vserver имя_vserver -role data
    ```

    где *имя_vserver* задает имя SVM. Полученное значение понадобится на шаге 6.
6. Задайте связанное средство перемещения данных для узла IBM Spectrum Protect, введя команду DEFINE DATAMOVER и задав параметр `TYPE=NASVSERVER`. На сервере IBM Spectrum Protect введите следующую команду в одной строке:

    ```
    define datamover имя_средства_перемещения_данных type=nasvserver
    hladdress=интерфейс_данных_svm lladdress=порт
    USER=имя_пользователя password=пароль dataformat=netappdump
    ```

    где *интерфейс_данных_svm* - это значение, которое вы получили в шаге 5, а *имя_средства_перемещения_данных* - это имя узла, зарегистрированное в шаге 4.

    Сведения о задании других параметров смотрите в разделе DEFINE DATAMOVER (Задать средство перемещения данных).

7. Сконфигурируйте политику сервера IBM Spectrum Protect для управления резервными копиями образов NAS. Следуйте инструкциям в разделе Конфигурирование политики IBM Spectrum Protect для операций NDMP.
8. Обновите узел, который вы зарегистрировали в шаге 4 для домена, сконфигурированного в шаге 7. На сервере IBM Spectrum Protect введите команду UPDATE NODE:

    ```
    update node имя_узла domain=имя_домена
    ```

9. (Необязательно): Определите тома в кластере и запланируйте операции резервного копирования. Выполните следующие шаги:
    a. На файл-сервере NAS укажите тома в кластере, введя следующую команду Data ONTAP:

    ```
    volume show -vserver имя_vserver
    ```

    где *имя_vserver* задает имя SVM.
    b. Запланируйте резервное копирование, выполнив инструкции в разделе Планирование операций NDMP.

Дальнейшие действия

Чтобы проверить, производится ли резервное копирование томов в кластере NetApp, выполните следующее:

1. В панели меню Центра операций выберите Клиенты.
2. Дважды щелкните по клиенту устройства NAS и щелкните по Тома.
3. Чтобы определить, когда было выполнено последнее полное резервное копирование тома, прочтите информацию в столбце Последнее полное. Чтобы определить, когда было выполнено последнее дифференциальное резервное копирование тома, прочтите информацию в столбце Последнее дифференциальное.

Ссылки, связанные с данной:
REGISTER NODE (Зарегистрировать узел)

Переконфигурирование IBM Spectrum Protect для оптимизации кластеризованного резервного копирования

Если вы сконфигурировали IBM Spectrum Protect для резервного копирования кластеров NetApp с использованием NDMP в области узлов, вы можете переконфигурировать IBM Spectrum Protect для использования NDMP Cluster Aware Backup (CAB). Это позволит оптимизировать операции резервного копирования для кластеров NetApp.

Прежде чем начать

Обзор функций NDMP в IBM Spectrum Protect и файл-серверов NetApp смотрите в техническом замечании 7046965. В этом техническом замечании также перечислены требования к системе.

Об этой задаче

Переконфигурируя IBM Spectrum Protect для использования CAB, вы можете оптимизировать операции резервного копирования следующими способами:

- Вы можете сконфигурировать IBM Spectrum Protect для резервного копирования всех томов в кластере NetApp на непосредственно подключенное ленточное устройство или на сервер IBM Spectrum Protect. В обоих случаях владельцем данных является один узел IBM Spectrum Protect. Даже если вы перемещаете тома в пределах кластера, резервное копирование продолжается, и переконфигурирование не требуется.
- Можно выполнить частичное резервное копирование кластера NetApp на сервер IBM Spectrum Protect. Этот метод полезен, если владельцами данных в кластере являются несколько организаций. Каждая организация может управлять операциями резервного копирования своих данных. Вы задаете эту область частичного резервного копирования, задавая виртуальную машину хранения (storage virtual machine, SVM) NetApp, которая обеспечивает доступ к части кластера.

Чтобы переконфигурировать IBM Spectrum Protect для использования CAB, нужно задать новый узел IBM Spectrum Protect и новое средство перемещения данных.

Процедура

1. Убедитесь, что на файл-сервере NetApp установлена операционная система NetApp Clustered Data ONTAP 8.2 или новее, или 9.1 или новее.
2. Включите использование NDMP, выполнив инструкции в публикации *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Выполните одно из следующих действий.

   Для полного резервного копирования кластера
   Сделайте следующее:
   a. Включите операции резервного копирования NDMP в области SVM на уровне кластера. Это позволит отключить операции резервного копирования NDMP в области узла на файл-сервере NAS. Убедитесь, что для опции node-scoped-ndmp на файл-сервере NAS задано значение OFF.
   b. Создайте резервный ID пользователя для операций NDMP.
   c. Сконфигурируйте сетевой интерфейс для управления соединениями NDMP на уровне кластера.

   Для частичного резервного копирования кластера
   Сделайте следующее:
   a. Включите NDMP в области SVM для управления операциями резервного копирования NDMP
   b. Создайте резервный ID пользователя для операций NDMP.
   c. Сконфигурируйте сетевой интерфейс для управления соединениями NDMP на уровне SVM.

3. Зарегистрируйте узел IBM Spectrum Protect, который будет владеть резервными копиями данных. На сервере IBM Spectrum Protect введите команду REGISTER NODE:

   ```
   register node имя_узла пароль
   domain=домен_nas type=nas
   ```

   где *имя_узла* - это имя узла, *пароль* - это пароль узла, а *домен_nas* - это домен узла.
4. Если вы собираетесь создать полную резервную копию кластера, определите IP-адрес интерфейса управления кластером NetApp на файл-сервере NAS. Интерфейс предоставляет доступ ко всему кластеру. На файл-сервере NAS введите следующую команду операционной системы Data ONTAP:

   ```
   network interface show -role cluster-mgmt
   ```

   IP-адрес, показаный в выходных результатах - это обязательное значение, если вы задали параметр HLADDRESS на шаге 6.
5. Если вы собираетесь создать резервную копию части кластера, определите цифровой IP-адрес либо имя домена интерфейса кластера, используемого SVM. Чтобы определить значение, введите на файл-сервере NAS следующую

команду операционной системы Data ONTAP:

```
network interface show -vserver имя_vserver -role data
```

где *имя_vserver* задает имя SVM. Полученное значение понадобится на шаге 6.

6. Задайте узел перемещения данных для узла IBM Spectrum Protect. Выполните одно из следующих действий.

   Для полного резервного копирования кластера
   Задайте узел перемещения данных для узла IBM Spectrum Protect, который станет владельцем резервной копии данных. На сервере IBM Spectrum Protect введите команду DEFINE DATAMOVER в одной строке:

   ```
   define
   datamover имя_средства_перемещения_данных type=nascluster
   hladdress=интерфейс_управления_кластером lladdress=порт
   USER=имя_пользователя password=пароль dataformat=netappdump
   ```

   где *интерфейс_управления_кластером* - это значение, которое вы получили на шаге 4, а *имя_средства_перемещения_данных* - это имя узла, зарегистрированное на шаге 3.
   Совет: После того как вы зададите средство перемещения данных, дополнительные средства перемещения данных будут автоматически заданы для каждого узла в кластере. Имя каждого средства перемещения данных соответствует имени физического узла в кластере. Вы будете использовать эти средства перемещения данных, когда будете задавать пути к ленточным накопителям, подключенным к кластеру.

   Для частичного резервного копирования кластера
   Задайте средство перемещения данных для узла, введя команду DEFINE DATAMOVER и задав параметр `TYPE=NASVSERVER`. На сервере IBM Spectrum Protect введите следующую команду в одной строке:

   ```
   define datamover
   имя_средства_перемещения_данных type=nasvserver
   hladdress=интерфейс_данных_svm lladdress=порт
   USER=имя_пользователя password=пароль dataformat=netappdump
   ```

   где *интерфейс_данных_svm* - это значение, которое вы получили в шаге 5, а *имя_средства_перемещения_данных* - это имя узла, зарегистрированное в шаге 3.

   Чтобы узнать, как задать другие параметры в команде DEFINE DATAMOVER, смотрите раздел DEFINE DATAMOVER (Задать средство перемещения данных).

7. Чтобы создать резервную копию данных на непосредственно подключенное ленточное устройство, для каждого ленточного накопителя, подключенного к кластеру, укажите имя устройства и физический узел, к которому подключается накопитель:
   a. На файл-сервере NAS введите следующую команду Data ONTAP:

      ```
      storage tape show-tape-drive
      ```

   b. Проверьте выходные данные, чтобы найти серийный номер ленточного накопителя и узел кластера, к которому подключен накопитель. В том же разделе будет и имя устройства, например, `st1`, `st2` или `st3`.
8. Чтобы сконфигурировать полное резервное копирование кластера на непосредственно подключенное ленточное устройство, следуйте инструкциям в разделе Конфигурирование ленточных устройств для полного резервного копирования кластера.
9. Чтобы сконфигурировать полное или частичное резервное копирование кластера на сервер IBM Spectrum Protect, сконфигурируйте политику управления резервными копиями образа NAS. Следуйте инструкциям в разделе Конфигурирование политики IBM Spectrum Protect для операций NDMP.
10. Отключите запланированные операции резервного копирования для всех узлов, которые ранее использовались для резервного копирования кластера NetApp.
11. Определите тома в кластере и (необязательно) запланируйте операции резервного копирования для томов. Выполните одно из следующих действий.

    Для полного резервного копирования кластера
    a. На файл-сервере NAS укажите тома в кластере при помощи следующей команды Data ONTAP:

       ```
       volume show
       ```

    b. Запустите полное резервное копирование всего кластера.
    c. (Необязательно): Чтобы запланировать операции резервного копирования, следуйте инструкциям в разделе Планирование операций NDMP.

    Для частичного резервного копирования кластера
    a. На файл-сервере NAS укажите тома в кластере при помощи следующей команды Data ONTAP:

```
volume show -vserver имя_vserver
```

где *имя_vserver* задает имя SVM.

b. Запустите полное резервное копирование части кластера.
c. (Необязательно): Чтобы запланировать операции резервного копирования, следуйте инструкциям в разделе Планирование операций NDMP.

Дальнейшие действия

Чтобы проверить, производится ли резервное копирование томов в кластере NetApp, выполните следующее:

1. В панели меню Центра операций выберите Клиенты.
2. Дважды щелкните по клиенту устройства NAS и щелкните по Тома.
3. Чтобы определить, когда было выполнено последнее полное резервное копирование тома, прочтите информацию в столбце Последнее полное. Чтобы определить, когда было выполнено последнее дифференциальное резервное копирование тома, прочтите информацию в столбце Последнее дифференциальное.

Ссылки, связанные с данной:
DEFINE DATAMOVER (Задать средство перемещения данных)
DEFINE PATH (Задать путь, когда пунктом назначения является накопитель)
REGISTER NODE (Зарегистрировать узел)

Резервное копирование и восстановление файл-серверов NAS с использованием NDMP

После того как вы сконфигурируете IBM Spectrum Protect для выполнения операций NDMP, вы будете готовы к тому, чтобы использовать NDMP.

Процедура

Для резервного копирования образа файловой системы используйте интерфейс клиента либо интерфейс администрирования. Например, чтобы использовать интерфейс клиента резервного копирования и архивирования Windows для резервного копирования файловой системы /vol/vol1 на файл-сервере NAS с именем NAS1, введите следующую команду:

```
dsmc backup nas -nasnodename=nas1 {/vol/vol1}
```

Дополнительную информацию об этой команде смотрите в разделе Резервное копирование образа.
Совет: Чтобы использовать интерфейс клиента для выполнения операций, необходимо пройти аутентификацию в качестве администратора IBM Spectrum Protect. У ID администратора должны быть полномочия на доступ к узлу NAS, как минимум, на уровне владельца клиента.
Эту же операцию можно выполнить с помощью серверного интерфейса. Например, при использовании клиента командной строки администрирования создайте резервную копию файловой системы /vol/vol1 на файл-сервере NAS с именем NAS1, введя следующую команду:

```
backup node nas1 /vol/vol1
```

Ограничение: Команды BACKUP NAS и BACKUP NODE не включают снимки. Чтобы узнать, как создавать резервные копии снимков, смотрите раздел Резервное копирование и восстановление с использованием снимков.
Восстановить образ можно, используя любой из двух интерфейсов. Резервные копии будут идентичными, независимо от того, с помощью какого интерфейса выполняется копирование - клиентского или серверного. Например, предположим, что вам нужно восстановить образ, резервная копия которого создавалась в предыдущих примерах. В этом примере файловая система с именем /vol/vol1 восстанавливается в /vol/vol2. Восстановите файловую систему с помощью следующей команды, введя ее в интерфейсе клиента резервного копирования и архивирования Windows:

```
dsmc restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}
```

Также файловую систему можно восстановить с помощью серверного интерфейса. Например, чтобы восстановить образ файловой системы с именем /vol/vol1 в файловую систему /vol/vol2 для файл-сервера NAS с именем NAS1, введите следующую команду:

```
restore node nas1 /vol/vol1 /vol/vol2
```

Можно восстановить данные с NAS-системы одного поставщика в NAS-систему другого, если используется формат данных NDMPDUMP. Однако необходимо либо проверить совместимость этих систем, либо поддерживать отдельный пул хранения для каждого поставщика NAS.

- Файл-серверы NAS: резервное копирование на один сервер IBM Spectrum Protect
  Если несколько файл-серверов NAS расположены в разных местах, может быть удобно передавать копируемые данные на один сервер IBM Spectrum Protect вместо того, чтобы подключать ленточную библиотеку к каждому устройству NAS.
- Резервное копирование файл-серверов NDMP на сервер IBM Spectrum Protect
  Можно создавать резервные копии данных на одном сервере IBM Spectrum Protect вместо того, чтобы подключать ленточную библиотеку к каждому устройству NAS.

Файл-серверы NAS: резервное копирование на один сервер IBM Spectrum Protect

Если несколько файл-серверов NAS расположены в разных местах, может быть удобно передавать копируемые данные на один сервер IBM Spectrum Protect вместо того, чтобы подключать ленточную библиотеку к каждому устройству NAS.

При сохранении данных резервных копий NAS в иерархии хранилища сервера IBM Spectrum Protect можно применять внутренние функции управления IBM Spectrum Protect. Это позволит вам воспользоваться преимуществами переноса, исправления, аварийного восстановления и другими функциями.

Чтобы выполнить резервное копирование устройства NAS в собственный пул хранения сервера IBM Spectrum Protect, настройте пул назначения таким образом, чтобы он указывал на нужный собственный пул хранения. Пул назначения содержит сведения о библиотеке и накопителях, используемых в операциях резервного копирования и восстановления. Следует убедиться, что в пуле назначения достаточно пространства для размещения данных NAS, резервные копии которых могут создаваться на устройствах с последовательным доступом, на дисковых устройствах, а также на устройствах типа File. Задаватьотдельный класс устройств не обязательно.

Если вы создаете содержание (TOC), в командах DEFINE и UPDATE COPYGROUP следует указывать класс управления при помощи параметра TOCDESTINATION. При резервном копировании файл-сервера NAS во внутренние пулы сервера IBM Spectrum Protect значение параметра TOCDESTINATION может совпадать с пунктом назначения данных, резервная копия которых создается с использованием NDMP.

Уровень безопасности для брандмауэра более высокий, чем при копировании с файлера в подключенную библиотеку, так как обмен информацией может быть инициирован как сервером IBM Spectrum Protect, так и файл-сервером NAS. Серверы лент NDMP работают как потоки на сервере IBM Spectrum Protect, и сервер лент принимает подключения к порту 10001. Этот номер порта можно изменить при помощи следующей опции в файле серверных опций IBM Spectrum Protect: NDMPPORTRANGE низший_номер_порта, высший_номер_порта.

При выполнении операций резервного копирования NDMP с файл-сервера на сервер можно использовать опцию NDMPPREFDATAINTERFACE, чтобы указать, какой сетевой интерфейс используется сервером IBM Spectrum Protect для получения данных резервных копий. Значением этой опции является имя хоста или адрес IPV4, связанный с одним из активных сетевых интерфейсов компьютера, на котором запущен сервер IBM Spectrum Protect. Для этого интерфейса должна быть включена поддержка протокола IPV4.

Прежде чем воспользоваться этой опцией, убедитесь, что устройство NAS поддерживает операции NDMP, использующие другой сетевой интерфейс для управляющих соединений NDMP и соединений NDMP для передачи данных. Управляющие соединения NDMP используются программой IBM Spectrum Protect для аутентификации на сервере NDMP и мониторинга операции NDMP, когда для передачи и приема данных резервных копий в ходе операций NDMP используются соединения NDMP для передачи данных. Устройство NAS необходимо настроить таким образом, чтобы оно направляло данные для резервного копирования и восстановления через соответствующий сетевой интерфейс.

Если опция NDMPPREFDATAINTERFACE задана, она повлияет на все последующие операции NDMP по передаче данных с файл-сервера на сервер. На управляющие соединения NDMP она не повлияет, так как они используют сетевой интерфейс системы по умолчанию. Эту опцию сервера можно изменять с помощью команды SETOPT без остановки и перезапуска сервера.

У файл-серверов NetApp есть опция NDMP (ndmpd.preferred_interface), позволяющая изменить интерфейс, используемый для соединений NDMP для передачи данных. Дополнительную информацию смотрите в документации по вашему устройству NAS.

Инструкции относительно выполнения операций резервного копирования с файл-сервера NDMP на сервер смотрите в разделе Резервное копирование файл-серверов NDMP на сервер IBM Spectrum Protect.

Информацию об опциях сервера для каждого продукта смотрите в разделе Опции сервера.

Резервное копирование файл-серверов NDMP на сервер IBM Spectrum Protect

Можно создавать резервные копии данных на одном сервере IBM Spectrum Protect вместо того, чтобы подключать ленточную библиотеку к каждому устройству NAS.

Процедура

Для резервного копирования сервера с файловой системой NAS надо выполнить следующие действия:

1. Выберите существующий пул хранения или сконфигурируйте пул хранения для данных NAS, введя следующую команду:

   ```
   define stgpool naspool disk
   ```

2. Определите тома и добавьте их в пул хранения. Например, определите том с именем naspool_volAB:

   ```
   define volume naspool /usr/storage/naspool_volAB formatsize=100
   ```

3. Настройте конечное расположение резервной копии в уже определенный пул хранения и активируйте связанный набор политик.

   ```
   update copygroup standard standard standard destination=naspool
    tocdestination=naspool
   activate policyset standard standard
   ```

   Конечное расположение данных NAS определяется конечным расположением в группе копий. Для оценки размера хранилища для дифференциальных резервных копий NAS используется уровень занятого файлового пространства; это же значение используется для полных резервных копий. Оценку размера можно использовать в качестве одного из критериев при выборе пула хранения. Одним из атрибутов пула хранения является значение MAXSIZE, указывающее, что данные передаются в следующий пул хранения (NEXT), если предполагаемый размер копируемых данных превышает значение MAXSIZE. Поскольку при дифференциальном резервном копировании NAS во внутренние пулы хранения на сервере IBM Spectrum Protect для оценки размера хранилища используется размер занятого базового файлового пространства, дифференциальные резервные копии заканчиваются в том же пуле хранения, что и полные резервные копии. В зависимости от настроек совместного размещения, дифференциальные копии могут заканчиваться на том же носителе, что и полные копии.
4. Настройте узел и устройство перемещения данных для устройства NAS. Формат данных указывает на то, что резервные копии, создаваемые данным устройством NAS, являются дампами резервной копии образа в специальном формате NetApp.

   ```
   register node nas1 nas1 type=nas domain=standard
   define datamover nas1 type=nas hla=nas1 user=root
   password=***** dataformat=netappdump
   ```

   Теперь устройство NAS готово к резервному копированию в пул хранения на сервере IBM Spectrum Protect. Хотя пути могут быть указаны к локальным накопителям, конечное расположение для операции резервного копирования определяется указанным в классе управления пулом назначения.
5. Выполните резервное копирование устройства NAS в пул хранения IBM Spectrum Protect с помощью следующей команды:

   ```
   backup node nas1 /vol/vol0
   ```

6. Восстановите устройство NAS из пула хранения IBM Spectrum Protect с помощью следующей команды:

   ```
   restore node nas1 /vol/vol0
   ```

Резервное копирование и восстановление на уровне файлов для операций NDMP

Когда вы производите резервное копирование данных с использованием NDMP, вы можете указать, что сервер IBM Spectrum Protect собирает и сохраняет информацию на уровне файлов в содержании (TOC).

Если указать этот параметр во время резервного копирования, позже можно будет просмотреть содержание (TOC) резервной копии образа. С помощью веб-клиента резервного копирования и архивирования версии 8.1.1 можно выбрать отдельные файлы или каталоги для восстановления непосредственно из созданных в результате резервного копирования образов.

Ограничение: Если вы установили клиент резервного копирования-архивирования V8.1.1 или ранее, то можно использовать интерфейс веб-клиента для операций восстановления уровня файла. Если вы установили клиент резервного копирования-архивирования V8.1.2 или новее, то использовать интерфейс веб-клиента для операций восстановления уровня файла нельзя.

Сбор сведений на уровне файлов требует дополнительного процессорного времени, сетевых ресурсов, пространства пула хранения, пространства для временной базы данных, а также, возможно, дополнительного взаимодействия с устройствами хранения. Инструкции по конфигурированию устройств хранения смотрите в разделе Конфигурирование устройств хранения. Нужно учитывать, что может потребоваться больше пространства в базе данных сервера IBM Spectrum Protect. Необходимо установить политику, согласно которой сервер IBM Spectrum Protect будет сохранять содержание (TOC) и резервную копию образа в разных пулах хранения. Содержание (TOC) обрабатывается так же, как и любой другой объект в данном пуле хранения.

Также можно выполнять операцию резервного копирования по NDMP без сбора сведений для восстановления на уровне файлов.

Чтобы разрешить создание содержания (TOC) для резервной копии, созданной с помощью NDMP, необходимо определить атрибут TOCDESTINATION в группе резервных копий для класса управления, к которому привязана данная резервная копия образа. В качестве пункта назначения нельзя указать пул хранения копий или пул активных данных. Указанный для размещения содержания пул хранения должен иметь формат данных NATIVE или NONBLOCK, поэтому он не может быть ленточным пулом хранения, используемым для хранения резервной копии образа.

Если необходимо собирать сведения на уровне файлов, нужно указать параметр TOC в серверной команде BACKUP NODE. Или же, если для операции резервного копирования используется клиент, можно указать параметр TOC в файле клиентских параметров, наборе клиентских параметров или клиентской командной строке. Можно указать значение NO, PREFERRED или YES. Если указать PREFERRED или YES, сервер IBM Spectrum Protect сохранит файловые сведения об одной управляемой NDMP резервной копии в содержании (TOC). Содержание (TOC) помещается в пул хранения. После этого сервер IBM Spectrum Protect получает доступ к содержанию (TOC), и сведения о файлах и каталогах могут быть запрошены сервером или клиентом. Использование параметра TOC позволяет создавать содержание (TOC) для отдельных конкретных образов, не задействуя для них другие классы управления.

Дополнительные сведения о команде BACKUP NODE смотрите в разделе BACKUP NODE (резервное копирование узла NAS).

Чтобы избежать задержек монтирования и обеспечить достаточный объем свободного пространства, в качестве пулов назначения для содержания (TOC), нужно использовать пулы хранения с произвольным доступом (класс устройств DISK). Для пулов хранения с последовательным доступом не требуется маркировка или другая подготовка томов, если разрешено использование чистых томов.

Дополнительную информацию смотрите в разделе Управление таблицами содержания.

- Интерфейсы для операций восстановления на уровне файлов
  Чтобы восстановить отдельные файлы и каталоги, можно использовать один из следующих интерфейсов: веб-клиент резервного копирования и архивирования версии 8.1.1 или более раней версии либо интерфейс сервера.
- Символы национальных языков для файл-серверов NetApp
  Все системы, создающие или использующие данные на отдельном томе файл-сервера NAS, должны выполнять такие операции в соответствии с установленным языком тома.
- Операции восстановления на уровне файлов из образа резервной копии на уровне каталогов
  Операции восстановления на уровне файлов поддерживаются для образов резервных копий на уровне каталогов.

Интерфейсы для операций восстановления на уровне файлов

Чтобы восстановить отдельные файлы и каталоги, можно использовать один из следующих интерфейсов: веб-клиент резервного копирования и архивирования версии 8.1.1 или более раней версии либо интерфейс сервера.

Ограничение: Если вы установили клиент резервного копирования-архивирования V8.1.1 или ранее, то можно использовать интерфейс веб-клиента для операций восстановления уровня файла. Если вы установили клиент резервного копирования-архивирования V8.1.2 или новее, то использовать интерфейс веб-клиента для операций восстановления уровня файла нельзя.

Рекомендации по использованию веб-клиента резервного копирования-архивирования V8.1.1 или ранее:

Чтобы восстановить файлы и каталоги, TOC должен существовать. Веб-клиент должен быть установлен на платформе Windows. Сервер IBM Spectrum Protect обращается к содержанию (TOC) из пула хранения и загружает сведения из содержания во временную таблицу базы данных. После этого можно воспользоваться веб-клиентом для просмотра каталогов и файлов, содержащихся в одном или нескольких образах файловых систем. Можно выбрать отдельные файлы или каталоги, чтобы восстановить данные непосредственно из сгенерированных образов резервных копий.

Рекомендации по использованию интерфейса сервера:

- Если у вас есть TOC, можно показать файлы в резервной копии при помощи команды QUERY TOC. При вводе команды RESTORE NODE укажите один или несколько файлов из выходной информации в параметре FILELIST.
- Если содержание (TOC) не было создано, увидеть содержание резервной копии образа будет нельзя. Вы сможете восстановить отдельные файлы и каталоги, если известны их имена и образ, в котором находится резервная копия. Воспользуйтесь командой RESTORE NODE с параметром FILELIST.

Символы национальных языков для файл-серверов NetApp

Все системы, создающие или использующие данные на отдельном томе файл-сервера NAS, должны выполнять такие операции в соответствии с установленным языком тома.

Для обеспечения полной поддержки символов мировых языков в именах файлов и каталогов на файл-сервере NetApp NAS необходимо установить пакет Data ONTAP 6.4.1 или более поздней версии.

Если версия Data ONTAP более ранняя, чем 6.4.1, то для сбора и восстановления сведений на уровне файлов необходима одна из следующих конфигураций. Результаты работы других конфигураций непредсказуемы. Во время операций резервного копирования сервер IBM Spectrum Protect генерирует сообщение с предупреждением (ANR4946W). Предупреждение указывает, что кодировка символов сообщений хронологии файлов NDMP неизвестна, а для построения содержания будет использоваться кодировка UTF-8. Это сообщение можно игнорировать только в следующих двух конфигурациях.

- Имена файлов и каталогов копируемых данных содержат только английские (7-битовые ASCII) символы.
- Имена файлов и каталогов копируемых данных содержат неанглоязычные символы, а язык тома установлен как UTF-8-версия для соответствующей локали (например, `de.UTF-8` для немецкого языка).

Если версия Data ONTAP 6.4.1 или более поздняя, то для сбора и восстановления сведений на уровне файлов необходима одна из трех следующих конфигураций. Результаты работы других конфигураций непредсказуемы.

- Имена файлов и каталогов копируемых данных содержат только английские (7-битовые ASCII) символы, а язык тома либо не задан, либо задано одно из следующих значений:
  - `C (POSIX)`
  - `en`
  - `en_US`
  - `en.UTF-8`
  - `en_US.UTF-8`
- Имена файлов и каталогов копируемых данных содержат неанглоязычные символы, а язык тома установлен как UTF-8-версия для соответствующей локали (например, `de.UTF-8` или `de` для немецкого языка).
  Совет: Использование UTF-8-версии языка тома более эффективно в плане обработки сервером IBM Spectrum Protect и пространства для содержания.
- CIFS используется исключительно для создания данных и работы с ними.

Операции восстановления на уровне файлов из образа резервной копии на уровне каталогов

Операции восстановления на уровне файлов поддерживаются для образов резервных копий на уровне каталогов.

Как и в случае резервного копирования файловой системы NAS, при резервном копировании на уровне каталогов создается содержание (Table of Contents - TOC). Файлы, содержащиеся в образе, можно просматривать с помощью веб-клиента версии 8.1.1 или более ранней версии. По умолчанию файлы восстанавливаются в исходное расположение. Однако для восстановления на уровне файлов из резервной копии уровня каталогов, в качестве конечного расположения можно выбрать другую файловую систему или другое имя виртуального файлового пространства.

Ограничение: Если вы установили клиент резервного копирования-архивирования V8.1.1 или ранее, то можно использовать интерфейс веб-клиента для операций восстановления уровня файла. Если вы установили клиент резервного копирования-архивирования V8.1.2 или новее, то использовать интерфейс веб-клиента для операций восстановления уровня файла нельзя.

В содержании образа резервной копии уровня каталогов имена всех файлов указываются относительно каталога, заданного в определении виртуального файлового пространства, а не корневого каталога файловой системы.

Операции резервного копирования и восстановления на уровне каталогов

Если используется большая файловая система NAS, резервное копирование на уровне каталогов позволит сократить время выполнения резервного копирования и восстановления и обеспечит больше гибкости при конфигурировании резервного копирования NAS. Путем определения виртуальных файловых пространств резервное копирование файловой системы можно разделить между несколькими операциями резервного копирования с помощью NDMP и несколькими ленточными накопителями. Также можно использовать различные расписания для резервного копирования поддеревьев файловой системы.

Имя виртуального файлового пространства не может совпадать с именем какой-либо файловой системы на узле NAS. Если на устройстве NAS создана файловая система с именем, которое уже носит виртуальная файловая система, на сервере IBM Spectrum Protect произойдет конфликт при создании резервной копии нового файлового пространства. Информацию о вводе команд для отображения виртуальных файловых пространств смотрите в разделе DEFINE VIRTUALFSMAPPING (Задать отображение виртуальных файловых пространств).
Ограничение: Отображения виртуальных файловых пространств поддерживаются только для узлов NAS.

- Резервное копирование и восстановление для операций NDMP
  Команда DEFINE VIRTUALFSMAPPING позволяет отобразить путь каталога на файл-сервере NAS в имя виртуального файлового пространства на сервере IBM Spectrum Protect. После того как отображение будет задано, вы сможете выполнять такие операции NAS, как BACKUP NODE и RESTORE NODE, используя имена виртуальных файловых пространств так же, как если бы они были настоящими файловыми пространствами NAS.
- Резервное копирование и восстановление с использованием снимков
  Операции резервного копирования NDMP на уровне каталогов позволяют выполнять резервное копирование созданных пользователями снимков файловой системы NAS. После этого снимки сохраняются как подкаталоги. Снимок можно сделать в любое время, а резервное копирование на ленту выполнить в более удобное время.

Резервное копирование и восстановление для операций NDMP

Команда DEFINE VIRTUALFSMAPPING позволяет отобразить путь каталога на файл-сервере NAS в имя виртуального файлового пространства на сервере IBM Spectrum Protect. После того как отображение будет задано, вы сможете выполнять такие операции NAS, как BACKUP NODE и RESTORE NODE, используя имена виртуальных файловых пространств так же, как если бы они были настоящими файловыми пространствами NAS.

Чтобы запустить резервное копирование каталога, введите команду BACKUP NODE и укажите имя виртуального файлового пространства вместо настоящего. Чтобы восстановить поддерево каталога туда, где оно находилось первоначально, введите команду RESTORE NODE, указав имя виртуального файлового пространства.

Определения виртуальных файловых пространств также можно указывать в команде RESTORE NODE в качестве пункта назначения. Таким способом можно восстанавливать резервные копии (как файловой системы, так и каталога) в каталог любой файловой системы устройства NAS.

Резервное копирование и восстановление с использованием снимков

Операции резервного копирования NDMP на уровне каталогов позволяют выполнять резервное копирование созданных пользователями снимков файловой системы NAS. После этого снимки сохраняются как подкаталоги. Снимок можно сделать в любое время, а резервное копирование на ленту выполнить в более удобное время.

Процедура

Например, чтобы выполнить резервное копирование снимка, созданного для файловой системы NetApp, сделайте следующее:

1. В консоли устройства NAS введите команду для создания снимка. В случае устройств NetApp это команда SNAP CREATE.

   ```
   snap create vol2 february17
   ```

   В этом примере создается снимок с именем FEBRUARY 17 файловой системы /vol/vol2. Физически данные снимка расположены в каталоге /vol/vol2/.snapshot/february17. Положение данных снимка зависит от реализации поставщика NAS. В случае устройств NetApp при помощи команды SNAP LIST можно вызвать на экран список всех снимков для файловой системы.
2. Создайте определение для сопоставления виртуального файлового пространства на сервере IBM Spectrum Protect для данных снимка, созданного на предыдущем этапе.

   ```
   define virtualfsmapping  nas1 /feb17snapshot  /vol/vol2  /.snapshot/february17
   ```

   В этом примере создается определение для сопоставления виртуального файлового пространства с именем /feb17snapshot.
3. Выполните резервное копирование сопоставления виртуального файлового пространства.

   ```
   backup node nas1 /feb17snapshot mode=full toc=yes
   ```

4. После создания резервной копии вы сможете восстановить весь образ снимка или отдельный файл. Перед тем как начать восстановление данных, можно создать имя сопоставления виртуального файлового пространства для каталога назначения. В качестве назначения можно выбрать любое имя файловой системы. Конечным расположением в данном примере является каталог /feb17snaprestore в файловой системе /vol/vol1.

   ```
   define virtualfsmapping  nas1 /feb17snaprestore  /vol/vol1  /feb17snaprestore
   ```

5. Восстановите образ резервной копии снимка.

   ```
   restore node nas1 /feb17snapshot /feb17snaprestore
   ```

   В этом примере восстанавливается копия файловой системы /vol/vol2 в папку /vol/vol1/feb17snaprestore в том же состоянии, в каком она была при создании снимка на первом этапе.

Операции резервного копирования и восстановления с использованием функции NetApp SnapMirror to Tape

Можно создать резервные копии больших файловых систем NetApp при помощи функции NetApp SnapMirror to Tape (она также называется SMTape). За счет использования при резервном копировании копии данных на уровне блоков, метод SnapMirror to Tape обеспечивает более высокую скорость, чем традиционное полное резервное копирование NDMP (Network Data Management Protocol), и может использоваться в тех случаях, когда полное резервное копирование NDMP является нерациональным.

Используйте функцию NDMP SnapMirror to Tape как вариант, обеспечивающий возможность аварийного восстановления, для копирования больших файловых систем NetApp в дополнительное хранилище. Для большинства файловых систем NetApp нужно использовать стандартный метод полного или дифференциального резервного копирования NDMP.

Задав параметр в командах BACKUP NODE и RESTORE NODE, вы сможете производить резервное копирование и восстановление файловых систем с использованием функции SnapMirror to Tape. Существует ряд ограничений по использованию образов SnapMirror. Прежде чем использовать эту функцию в качестве метода резервного копирования, примите во внимание следующие рекомендации:

- Если вы установили NetApp ONTAP 8.2 или новее, вы должны задать средство перемещения данных типа NASCLUSTER или NASVSERVER для операций SnapMirror to Tape.
- Нельзя инициировать операцию резервного копирования или восстановления SnapMirror на ленту из IBM Spectrum Protect Центр операций, Web-клиента или клиента командной строки.

- Производить дифференциальное резервное копирование образов SnapMirror нельзя.
- Производить резервное копирование на уровне каталогов с использованием SnapMirror to Tape нельзя. Поэтому IBM Spectrum Protect не разрешает выполнение операций резервного копирования SnapMirror to Tape в виртуальном файловом пространстве сервера.
- Выполнять операции восстановления NDMP на уровне файлов с использованием образов SnapMirror to Tape нельзя. Поэтому при создании резервных копий образов SnapMirror to Tape содержание (TOC) никогда не создается.
- В начале операции копирования SnapMirror to Tape файл-сервер генерирует снимок файловой системы. В NetApp имеется переменная среды NDMP, которая позволяет указать, следует ли удалить этот снимок в конце операции SnapMirror to Tape. IBM Spectrum Protect всегда задает эту переменную, так чтобы снимок удалялся.
- После того, как образ SnapMirror to Tape будет получен и скопирован в систему NetApp, файловая система назначения останется сконфигурированной в качестве партнера SnapMirror. В NetApp имеется переменная среды NDMP, которая позволяет указать, следует ли разорвать эту взаимосвязь SnapMirror. IBM Spectrum Protect всегда разрывает взаимосвязь при получении данных SnapMirror. По завершении восстановления файловая система назначения окажется в том же состоянии, в каком находилась исходная файловая система в момент резервного копирования.

Дополнительную информацию о функции SnapMirror to Tape смотрите в разделах BACKUP NODE (резервное копирование узла NAS) и RESTORE NODE (восстановление узла NAS).

Операции резервного копирования NDMP с использованием интегрированных с файл-сервером контрольных точек Celerra

Когда сервер IBM Spectrum Protect инициирует операцию резервного копирования NDMP на устройстве перемещения данных Celerra, для выполнения резервного копирования большой файловой системы может потребоваться несколько часов. Без интегрированных контрольных точек Celerra все изменения, происходящие в файловой системе, будут записаны в резервную копию образа.

В результате резервная копия образа будет содержать изменения, которые вносились в файловую систему на всем протяжении операции резервного копирования. Резервная копия образа не является истинным образом точки во времени для файловой системы.

Если вы выполняете операции резервного копирования NDMP для файл-серверов Celerra, обновите операционную систему устройства перемещения данных до файл-сервера Celerra версии T5.5.25.1 или новее. Эта версия операционной системы обеспечивает поддержку интегрированных контрольных точек для всех операций резервного копирования NDMP, запускаемых с управляющей рабочей станции Celerra. Включив эту функцию, вы получите гарантию того, что данные резервной копии будут соответствовать истинным моментальным образам файловой системы, резервное копирование которой производится.

Инструкции относительно того, как включить интегрированные контрольные точки при выполнении всех операций резервного копирования NDMP, смотрите в документации по файл-серверу Celerra.

Если операционная система файл-сервера Celerra относится к более раннему уровню, чем версия T5.5.25.1, и если вы используете NDMP для резервного копирования устройств перемещения данных Celerra, сгенерируйте вручную снимок файловой системы с использованием функции контрольной точки командной строки Celerra. Затем инициируйте операцию резервного копирования NDMP контрольной точки файловой системы, а не исходной файловой системы.

Инструкции по созданию и планированию контрольных точек с управляющей рабочей станции Celerra смотрите в документации по файл-серверу Celerra.

Репликация узлов NAS

Вы можете реплицировать узел NAS, для которого используется NDMP при выполнении операций резервного копирования. Прежде чем конфигурировать операцию репликации, прочтите информацию о действующих ограничениях.

Об этой задаче

ограничения:

- Данные резервных копий должны находиться в пуле хранения с форматом данных NATIVE. Реплицировать данные резервных копий в пулах хранения с указанными ниже форматами нельзя:
  - NETAPPDUMP

    - CELERRADUMP
    - NDMPDUMP
- Дифференциальную резервную копию можно реплицировать, только если реплицируется соответствующая полная резервная копия.

Процедура

1. Включите узел NAS для репликации, введя команду UPDATE NODE:

   ```
   update node имя_узла replstate=enabled
   ```

   где *имя_узла* задает имя узла NAS.
2. Реплицируйте узел, введя команду REPLICATE NODE:

   ```
   replicate node имя_узла
   ```

   где *имя_узла* задает имя узла NAS.
3. Чтобы убедиться, что реплицированные данные можно восстановить, задайте на целевом сервере средство перемещения данных для узла, введя команду DEFINE DATAMOVER:

   ```
   define datamover имя_узла type=nas hladdress=адрес_hl
   lladdress=адрес_ll
       userid=id_пользователя password=пароль_пользователя dataformat=netappdump
   ```

   Здесь используются следующие обозначения:

   имя_узла
   : Задает имя узла NAS.

   адрес_hl
   : Задает либо цифровой IP-адрес, либо имя домена, используемые для доступа к файл-серверу NAS.

   адрес_ll
   : Задает номер порта TCP для доступа к устройству NAS для сеансов NDMP.

   id_пользователя
   : Задает ID пользователя, авторизованного для инициирования сеанса NDMP с использованием файл-сервера NAS.

   пароль_пользователя
   : Задает пароль пользователя, авторизованного для инициирования сеанса NDMP с использованием файл-сервера NAS.

Результаты

Формат данных резервных копий не изменяется в процессе репликации. При репликации данных резервных копий также реплицируется и связанное с ним содержание (TOC).

Защита данных с использованием лицензированной функции NetApp SnapLock

Лицензированную функцию NetApp SnapLock можно использовать, чтобы выполнить строгие нормативные требования для заархивированных данных. При включении функции SnapLock можно использовать IBM Spectrum Protect, чтобы задать срок хранения файлов и перевести файл в состояние WORM (Write Once Read Many).

Данные, хранящиеся с заданным сроком хранения, нельзя удалить из файловой системы, прежде чем истечет срок хранения. Функцию SnapLock могут использовать только серверы IBM Spectrum Protect, если на них включена защита хранения данных.

Данные, архивируемые серверами с защитой хранения и сохраненные на файл-серверах NetApp NAS, хранятся как тома FILE IBM Spectrum Protect. В конце транзакции записи для тома FILE устанавливается дата срока хранения через интерфейс SnapLock. Эта дата вычисляется с использованием параметров RETVER и RETMIN группы архивных копий, которая используется вами при архивировании данных. Если связать дату хранения с томом FILE, том FILE не уничтожит и не перезапишет данные, пока не пройдет срок хранения. Такие тома FILE называются томами WORM FILE. После того как будет задана дата хранения, том WORM FILE нельзя будет удалить, пока не пройдет срок хранения. Программа IBM Spectrum Protect for Data Retention в сочетании с высвобождением томов WORM FILE обеспечивает защиту в течение всего срока хранения данных.

Пулы хранения могут управляться либо порогом, либо сроком хранения данных. Параметр RECLAMATIONTYPE пула хранения указывает, что пул хранения управляется на основании срока хранения данных. Если информация из обычного пула хранения запрашивается с использованием параметра FORMAT=DETAILED, появится следующая выходная информация:

```
Reclamation Type: THRESHOLD
```

Если на сервере IBM Spectrum Protect включена защита хранения данных при помощи IBM Spectrum Protect for Data Retention и у сервера есть доступ к файл-серверу NetApp с лицензированной функцией SnapLock, вы можете задать пул хранения, задав для параметра RECLAMATIONTYPE значение SNAPLOCK. Это означает, что данные, созданные на томах в этом пуле хранения, управляются датой хранения. При запросе информации из пула хранения SnapLock с использованием параметра FORMAT=DETAILED в выходной информации будет указано, что пулы хранения управляются сроком хранения данных:

```
 Тип высвобождения: SNAPLOCK
```

Более подробную информацию о файл-сервере SnapLock смотрите в документации по NetApp *Data ONTAP Archive and Compliance Management Guide for 7-Mode* (Руководство по управлению архивированием и совместимостью ONTAP данных).

Внимание: Не используйте эту функцию для защиты данных со сроком хранения менее трех месяцев.

- Высвобождение пространства и функция SnapLock
  Чтобы убедиться, что данные всегда защищены, задайте срок хранения по умолчанию в NetApp, равный 30 дням, чтобы он соответствовал сроку высвобождения пространства по умолчанию на томе WORM FILE. IBM Spectrum Protect произведет консолидацию всех оставшихся на томе WORM FILE данных непосредственно перед истечением срока хранения.
- Сроки хранения
  Политики IBM Spectrum Protect управляют временем сроков хранения тома WORM FILE. Срок хранения некоторых файлов может превышать время хранения для тома WORM FILE, на котором они хранятся. Возможно, вам придется переместить некоторые файлы на другой том, чтобы файлы хранились на носителях WORM.
- Конфигурация функции SnapLock для хранения на основе событий
  Данные, которые хранятся на томах SnapLock и которыми управляет компонент IBM Spectrum Protect for Data Retention, а также хранение на основе событий могут вызвать избыточное высвобождение пространства, из-за чего снизится производительность сервера.
- Постоянная защита данных с использованием функции SnapLock
  Если данные хранятся на томе с включенной функцией SnapLock и данные переместят или скопируют на том, не являющийся томом SnapLock, данные потеряют уникальную аппаратную защиту, обеспечиваемую томами NetApp WORM.
- Настройка томов SnapLock как томов IBM Spectrum Protect WORM FILE
  Чтобы выполнить строгие требования к заархивированным данным, включите функцию NetApp SnapLock.

Высвобождение пространства и функция SnapLock

Чтобы убедиться, что данные всегда защищены, задайте срок хранения по умолчанию в NetApp, равный 30 дням, чтобы он соответствовал сроку высвобождения пространства по умолчанию на томе WORM FILE. IBM Spectrum Protect произведет консолидацию всех оставшихся на томе WORM FILE данных непосредственно перед истечением срока хранения.

Высвобождение тома WORM FILE на другой том WORM FILE до истечение даты хранения поможет убедиться, что данные всегда защищены функцией SnapLock.

Поскольку защита всегда устанавливается на уровне томов IBM Spectrum Protect, данными на томе можно управлять с помощью политики IBM Spectrum Protect, не принимая во внимание, где хранятся данные. Данные, хранящиеся на томах WORM FILE, защищены как защитой хранения данных, так и сроком хранения, сохраненным вместе с физическим файлом на томе SnapLock. Если администратор IBM Spectrum Protect введет команду удаления данных, команда завершится неудачно. Если кто-либо попытается удалить файл, имспользуя серию вызовов сетевой файловой системы, функция SnapLock не позволит удалить данные.

Если при освобождении пространства серверу IBM Spectrum Protect не удастся переместить данные с устаревающего тома на новый том SnapLock, появится предупреждение.

Сроки хранения

Политики IBM Spectrum Protect управляют временем сроков хранения тома WORM FILE. Срок хранения некоторых файлов может превышать время хранения для тома WORM FILE, на котором они хранятся. Возможно, вам придется переместить некоторые файлы на другой том, чтобы файлы хранились на носителях WORM.

Может потребоваться, чтобы некоторые объекты тома хранились дольше, чем другие, по таким причинам:

- Объекты связаны с классами управления с разными сроками хранения.
- Объекты нельзя удалить из-за задержки удаления.
- Объекты ожидают события, после которого должны устареть.
- Срок хранения для группы копии увеличивается, для чего требуется более длительное времени хранения, чем время, заданное в компоненте SnapLock, когда осуществлялся прием тома WORM FILE.

Чтобы управлять томом WORM FILE на основе времени хранения, нужно ввести команду DEFINE STGPOOL и задать параметр RECLAMATIONTYPE=SNAPLOCK. Это позволит задать пул хранения как пул хранения SnapLock. После этого вы не сможете обновить параметр RECLAMATIONTYPE, присвоив ему значение THRESHOLD. Когда вы задаете пул хранения SnapLock, система проверяет, являются ли указанные каталоги в классе устройств томами SnapLock WORM. При создании определения класса устройств FILE и создании пулов хранения с типом консолидации пространства SNAPLOCK все тома должны быть томами WORM, иначе операция завершится неудачно. Если класс устройств обновляется, так чтобы он содержал дополнительные каталоги, и пулы хранения SnapLock назначаются для класса устройств, производится такая же проверка, чтобы убедиться, что все каталоги являются томами SnapLock WORM.

Для функции NetApp SnapLock доступны три срока хранения. Сроки хранения нужно сконфигурировать правильно, так чтобы сервер IBM Spectrum Protect смог правильно управлять данными WORM, хранящимися на томах SnapLock. Сервер IBM Spectrum Protect задает срок хранения для данных, хранящихся на томах NetApp SnapLock, на основе зрачений в группе копий для архивируемых данных. Файл-сервер NetApp не должен вступать в конфликт с сервером IBM Spectrum Protect в отношении назначения срока хранения. Предпочтительный метод - сконфигурировать на файл-сервере NetApp следующие параметры для сроков хранения:

- Минимальный срок хранения. Задайте более высокое значение: либо 30 дней, либо минимальный срок в днях, заданный любой группой копий (с использованием файл-сервера NetApp SnapLock для хранения WORM FILE) для срока хранения данных. Группа копий - это группа, которая используется для сохранения данных на томах NetApp SnapLock.
- Максимальный срок хранения. Оставьте без изменения значение по умолчанию, равное 30 годам. Этот срок хранения позволит серверу IBM Spectrum Protect задать фактический срок хранения томов на основании параметров группы архивных копий.
- Срок хранения по умолчанию. Задайте 30 дней. Если вы не зададите это значение и не зададите максимальный срок хранения, для каждого тома будет задан срок хранения, равный 30 годам. Если это произойдет, сервер IBM Spectrum Protect не сможет управлять устареванием томов NetApp SnapLock и использовать их повторно. В результате этого никакие тома нельзя будет повторно использовать в течение 30 лет.

Если сроки хранения NetApp SnapLock заданы, IBM Spectrum Protect сможет управлять данными в пулах хранения SnapLock с максимальной эффективностью. Для каждого тома в пуле хранения SNAPLOCK создается период консолидации пространства IBM Spectrum Protect. У периода консолидации пространства IBM Spectrum Protect есть дата начала — BEGIN RECLAIM PERIOD, и дата окончания — END RECLAIM PERIOD. Можно просмотреть эти даты, введя для тома SnapLock команду QUERY VOLUME с параметром FORMAT=DETAILED. Результат выполнения команды выглядит, как в следующем примере:

```
Начало периода консолидации: 09/05/2017
  Завершение периода консолидации: 10/06/2017
```

Когда IBM Spectrum Protect архивирует файлы на том SnapLock, сервер отслеживает последнюю дату устаревания этих файлов, и в качестве значения BEGIN RECLAIM PERIOD будет задана последняя дата устаревания. При добавлении на том SnapLock дополнительных файлов для начальной даты будет задана эта более поздняя дата, если у вас есть файл с более поздней датой устаревания, чем у того, который находится сейчас на томе. Датой начала устанавливается последняя дата устаревания одного из файлов тома. Ожидается, что все файлы на этом томе либо уже истекли, либо истекают в этот день. На следующий день на этом томе не останется никаких действительных данных.

Для END RECLAIM PERIOD будет задан месяц, наступающий после BEGIN RECLAIM PERIOD. Дата хранения, заданная на файл-сервере NetApp для этого тома, будет назначена датой END RECLAIM PERIOD. Файл-сервер NetApp запрещает удалять этот том, пока не наступит дата END RECLAIM PERIOD. Эта дата представляет собой примерно месяц после истечения срока действия данных на сервере IBM Spectrum Protect. Если сервер IBM Spectrum Protect вычисляет дату END RECLAIM PERIOD для тома и эта дата окажется позже текущего значения END RECLAIM PERIOD, дата для этого тома переустанавливается на файл-сервере NetApp на более позднюю дату. Переустановка даты на более позднюю дату

гарантирует, что том IBM Spectrum Protect WORM FILE не удаляется, пока не истечет срок действия всех данных на этом томе или пока данные не будут перемещены на другой том SnapLock.

Период консолидации пространства IBM Spectrum Protect - это время между датой начала и датой окончания. Во время периода консолидации сервер IBM Spectrum Protect удаляет тома, на которых истек срок действия всех данных, или перемещает файлы, срок действия которых на истекающих томах SnapLock не окончился, на новые тома SnapLock с новыми датами. Этот месяц важен для безопасности и эффективности управления данными на сервере в томах WORM FILE. Данные на томе SnapLock, как правило, истекают, когда наступает начальная дата, и том должен быть пустым. Когда наступает конечная дата, том можно спокойно удалить из перечня IBM Spectrum Protect и с файл-сервера SnapLock.

Однако некоторые события могут вызвать появление действительных данных на томе SnapLock:

- Обработка устаревания на сервере IBM Spectrum Protect для этого тома могла быть задержана или не завершилась полностью.
- Параметры хранения для группы копий или связанных классов управления могли быть изменены для файла после его архивирования, и срок действия этого файла не должен скоро истечь.
- Могло быть установлено удерживание удаления для одного или нескольких файлов на томе.
- Либо выключена обработка консолидации (высвобождения) пространства, либо были обнаружены ошибки при перемещении данных на новые тома SnapLock в пуле хранения SnapLock.
- Файл ожидает события, прежде чем сервер IBM Spectrum Protect сможет начать процесс удаления устаревших файлов.

Когда наступает начальная дата и срок действия файлов не истекает на томе SnapLock, файлы могут быть перемещены на новый том SnapLock с новыми начальными и конечными датами. Однако, если обработка устаревания на сервере IBM Spectrum Protect отложена и срок действия этих файлов заканчивается, когда выполняется обработка устаревания на сервере IBM Spectrum Protect, перемещать эти файлы на новый том SnapLock неэффективно. Чтобы убедиться, что ненужное перемещение файлов не происходит для файлов, срок действия которых должен закончиться, перемещение файлов на истекающих томах SnapLock будет задержано на определенное число дней после даты BEGIN RECLAIM PERIOD. Поскольку данные на файл-сервере SnapLock защищены до наступления даты END RECLAIM PERIOD, задержка этого перемещения не несет никакого риска для данных. Это позволяет обработке устаревания IBM Spectrum Protect завершиться. По истечении этого числа дней, если на истекающем томе SnapLock есть действительные данные, данные будут перемещены на новый том SnapLock, что позволяет продолжить защиту данных.

Поскольку данные были первоначально заархивированы, могли произойти изменения параметров хранения для этих данных (например, изменения класса управления или параметров пула копий) или для этих данных могло быть установлено удерживание удаления. Однако данные на этом томе защищены компонентом SnapLock только до наступления даты END RECLAIM PERIOD. Данные, срок действия которых не закончился, перемещаются на новые тома SnapLock во время периода консолидации IBM Spectrum Protect. Если при перемещении данных на новый том SnapLock произойдут ошибки, будет сгенерировано сообщение с предупреждением, где будет указано, что данные скоро станут незащищенными. Если ошибка повторится, введите команду MOVE DATA для проблемного тома.

Внимание: Не выключайте обработку консолидации в пуле хранения SnapLock. После выключения обработки у сервера IBM Spectrum Protect не будет никакой возможности сгенерировать сообщения с предупреждениями о том, что данные станут незащищенными. Такая ситуация также может возникнуть, если консолидация и перенос выключены для всего сервера (например, в файле опций сервера задан параметр NOMIGRRECL). При управлении пулами хранения SnapLock убедитесь, что ваши данные защищены.

Конфигурация функции SnapLock для хранения на основе событий

Данные, которые хранятся на томах SnapLock и которыми управляет компонент IBM Spectrum Protect for Data Retention, а также хранение на основе событий могут вызвать избыточное высвобождение пространства, из-за чего снизится производительность сервера.

Если данные управляются хранением на основе событий, IBM Spectrum Protect первоначально задаст в качестве срока хранения большее из значений RETVER и RETMIN для группы архивных копий. Когда для тома подходит период высвобождения и оставшиеся на томе данные перемещаются, в качестве срока хранения для тома назначения будет задан оставшийся срока хранения данных, который, как правило, равен 0. После этого для нового тома подойдет период высвобождения, вскоре после того как том получит данные, из-за чего произойдет высвобождение только что созданных томов.

Этого можно избежать, если использовать серверную опцию RETENTIONEXTENSION. Эта опция позволяет серверу установить или продлить дату срока хранения тома SnapLock. Введите значение от 30 до 9999 дней. Значение по умолчанию равно 365.

Когда вы выбираете тома в пуле хранения SnapLock для высвобождения пространства, сервер проверяет, наступил ли для тома период высвобождения:

- Если период высвобождения тома не начался, ничего не произойдет. Пространство на томе не будет высвобождаться, и дата хранения не изменится.
- Если для тома подошел период высвобождения, сервер проверит, будет ли процент высвобождаемого пространства на томе выше, чем порог высвоождения для пула хранения или порог в процентах, переданный в параметре THRESHOLD команды RECLAIM STGPOOL:
    - Если пространство, подлежащее высвобождению, не превышает порог, сервер высвободит пространство на томе и задаст для тома назначения срок хранения, равный большему из следующих значений:
        - Оставшийся срок хранения данных плюс 30 дней для периода высвобождения пространства.
        - Значение RETENTIONEXTENSION плюс 30 дней для периода высвобождения пространства.
    - Если пространство, подлежащее высвобождению, не превышает порог, сервер переустановит срок хранения тома на значение, заданное опцией RETENTIONEXTENSION. Новый срок хранения вычисляется путем прибавления заданного числа дней к текущей дате.

В следующих примерах том SnapLock, VolumeA, находится в пуле хранения, для которого в качестве порога высвобождения пространства задано значение 60%. Для серверной опции RETENTIONEXTENSION задано значение, равное 365 дням. Срок хранения для тома VolumeA находится в пределах срока высвобождения. Следующие ситуации показывают, что происходит со сроком хранения.

- Подлежащее высвобождению пространство на томе VolumeA, составляет менее 60%. Окончание срока хранения для тома VolumeA продлевается на 365 дней.
- Подлежащее высвобождению пространство на томе VolumeA, составляет более 60%, а оставшаяся часть срока хранения данных больше 365 дней. Том VolumeA будет высвобожден, и для тома назначения будет задан срок хранения на основе оставшегося срока хранения плюс 30 дней для срока высвобождения.
- Подлежащее высвобождению пространство на томе VolumeA, составляет более 60%, а оставшаяся часть срока хранения данных менее 365 дней. Том VolumeA будет высвобожден, и для него будет задан срок хранения, равный 365 дням (это значение опции RETENTIONEXTENTION) плюс 30 дней для периода консолидации остаточных данных.

Постоянная защита данных с использованием функции SnapLock

Если данные хранятся на томе с включенной функцией SnapLock и данные переместят или скопируют на том, не являющийся томом SnapLock, данные потеряют уникальную аппаратную защиту, обеспечиваемую томами NetApp WORM.

Сервер IBM Spectrum Protect разрешает такой тип перемещений. Однако, если данные окажутся перемещены с тома WORM FILE на другой тип носителя, данные могут быть больше не защищены от случайного или умышленного удаления. не будут защищены от случайного или умышленного удаления. Если данные на томах WORM используются для выполнения требований к хранению данных и защите с целью соблюдения юридических требований и перемещаются на другой носитель, данные могут больше не соответствовать этим требованиям. Вы должны сконфигурировать пулы хранения, так чтобы этот тип данных оставался в пулах хранения, состоящих из томов SnapLock WORM, в течение всего срока хранения данных.

Настройка томов SnapLock как томов IBM Spectrum Protect WORM FILE

Чтобы выполнить строгие требования к заархивированным данным, включите функцию NetApp SnapLock.

Об этой задаче

Когда вы задаете или обновляете конфигурации, в которых есть пулы хранения SnapLock, убедитесь, что задана опция RECLAMATIONTYPE=SNAPLOCK для пулов хранения, выбранных для параметров NEXTSTGPOOL, RECLAIMSTGPOOL и COPYSTGPOOLS.

Конфигурируя пулы хранения подобным образом, вы сможете убедиться, что данные правильно защищены. Если вы зададите следующий пул, пул высвобождения, пул хранения копий или пул активных данных, не выбирая опцию RECLAMATIONTYPE=SNAPLOCK, пул хранения не будет защищен. Команда будет выполнена с предупреждением.

Процедура

Чтобы настроить том SnapLock для использования в качестве тома WORM FILE IBM Spectrum Protect, выполните следующие шаги:

1. Установите и настройте SnapLock на файл-сервере NetApp. Убедитесь, что вы сконфигурировали минимальный, максимальный периоды хранения и период хранения по умолчанию. Инструкции смотрите в документации по NetApp.
2. Установите и сконфигурируйте сервер IBM Spectrum Protect.
3. Включите защиту хранения архивных данных, введя команду SET ARCHIVERETENTIONPROTECTION:

   ```
   set archiveretentionprotection on
   ```

4. Задайте политику при помощи команды DEFINE COPYGROUP. Выберите значения RETVER и RETMIN в группе архивных копий, соответствующей вашим требованиям к защите этих данных в хранилище WORM. Если значения RETVER или RETMIN не заданы, будут использоваться значения классов управления по умолчанию.
5. Настройте хранилище, используя команду DEFINE DEVCLASS.
   - Используйте класс устройств FILE.
   - Задайте параметр DIRECTORY, чтобы указать каталог или каталоги на томах SnapLock.
6. Задайте пул хранения, используя класс устройств, заданный в шаге 5, введя команду DEFINE STGPOOL и задав параметр RECLAMATIONTYPE=SNAPLOCK.
7. Обновите группу копий, так чтобы она указывала на пул хранения; для этого введите команду UPDATE COPYGROUP.
8. Используя API IBM Spectrum Protect, заархивируйте объекты в пул хранения SnapLock. Для стандартных клиентах резервного копирования и архивирования IBM Spectrum Protect эта функция недоступна.

Восстановление данных

Можно исправить поврежденные экстенты данных в пулах хранения каталогов-контейнеров и восстановить потерянные данные после аварии.

Экстент данных - это часть файла, созданного в процессе дедупликации данных. Экстенты сравниваются с экстентами других файлов с целью идентификации дубликатов. Если у вас есть поврежденные файлы или каталоги в пуле хранения каталогов-контейнеров, можно исправить экстенты дедуплицированных данных с сервера репликации назначения, исходного сервера репликации, а также из ленточных томов пула хранения контейнеров-копий.

- Восстановление пулов хранения с целевого сервера репликации
  Если файлы, каталоги или пулы хранения на исходном сервере репликации повреждены, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров на исходном сервере репликации с сервера репликации назначения.
- Восстановление пулов хранения с томов пула хранения контейнеров-копий
  Если файлы, каталоги или пулы хранения на исходном сервере повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на исходном сервере путем извлечения экстентов дедуплицированных данных из локальных или удаленных ленточных томов пулов хранения контейнеров-копий.
- Исправление пулов хранения в среде с сервером репликации и томами пула хранения контейнеров-копий
  Если файлы, каталоги или пулы хранения на исходном сервере повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на исходном сервере репликации путем извлечения экстентов дедуплицированных данных с сервера репликации назначения или из ленточных томов пулов хранения контейнеров-копий.
- Исправление пулов хранения на сервере репликации назначения
  Если файлы, каталоги или пулы хранения на сервере репликации назначения повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на сервере репликации назначения путем извлечения экстентов дедуплицированных данных с исходного сервера репликации.
- Восстановление пулов хранения после аварии
  Можно восстановить пулы хранения каталогов-контейнеров и возвратить их потерянные данные после аварии.
- Замена поврежденного ленточного тома пула хранения контейнеров-копий
  Если ленточный том, в котором хранятся копии дедуплицированных экстентов данных пула хранения контейнеров-копий, поврежден, можно заменить этот том.

Понятия, связанные с данным:
Стратегии для защиты при авариях
Задачи, связанные с данной:
Решения для защиты данных
Восстановление от потери данных или системных отключений электричества

Восстановление пулов хранения с целевого сервера репликации

Если файлы, каталоги или пулы хранения на исходном сервере репликации повреждены, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров на исходном сервере репликации с сервера репликации назначения.

Прежде чем начать

Сделайте следующее:

1. Оцените свою среду хранения и решите, что происходит в результате отключений питания, сетевых проблем и отказов оборудования: данные повреждаются или данные выглядят поврежденными. Если проблемы в вашей среде приводят к повреждению данных, найдите и исправьте эти проблемы.
2. Убедитесь, что в пуле хранения каталогов-контейнеров достаточно доступного пространства для восстановленных данных. Параметр PREVIEW=YES в команде REPAIR STGPOOL задает объем данных, которые будут исправлены. Если места недостаточно, воспользуйтесь командой DEFINE STGPOOLDIRECTORY для выделения пространства.
3. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
4. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
5. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
     b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
     c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить повреждения следующих типов:

- Незначительные повреждения, вызванные случайным удалением файлов или каталогов, перезаписью файлов, случайным изменением разрешений для файла или ошибками диска в связи с аппаратными проблемами.
- Умеренные повреждения, вызванные ошибками диска или ошибками монтирования диска. Такое повреждение приводит к потере одного или нескольких каталогов, но не к потере всего пула хранения.

Поврежденные дедуплицированные экстенты восстанавливаются по экстентам, которые были защищены на сервере репликации назначения.
Ограничение: Команду REPAIR STGPOOL для заданного пула хранения можно ввести, только если вы уже скопировали данные в другой пул хранения на сервере репликации назначения при помощи команды PROTECT STGPOOL.
При исправлении пула хранения каталога-контейнера с сервера репликации команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Целевой сервер репликации недоступен.

- Целевой пул хранения поврежден.
- Произошло отключение сети.

Процедура

1. Если вы подозреваете небольшое повреждение, введите команду AUDIT CONTAINER для пула хранения контейнеров на уровне каталога, чтобы выявить несогласованности между базой данных и пулом хранения каталогов-контейнеров. Выявив поврежденные экстенты данных в пуле хранения каталогов-контейнеров, вы сможете определить, какие экстенты данных следует исправить. Для сбережения времени и ресурсов выполняйте аудит только для контейнеров с подозрениями на повреждения. Если вы предполагаете, что ваш пул хранения каталогов-контейнеров имеет более серьезные повреждения, введите команду AUDIT CONTAINER на уровне пула хранения.
   Например, для выполнения аудита каталога n:\pooldir в пуле хранения с именем STGPOOL1 введите команду:

   ```
   audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
   ```

   Для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

   ```
   audit container stgpool=stgpool1
   ```

   Процесс аудита может выполняться несколько часов.

2. Для исправления пула хранения каталогов-контейнеров введите команду REPAIR STGPOOL и задайте параметр SRCLOCATION=REPLSERVER. Например, для исправления пула хранения с именем STGPOOL1 с сервера репликации введите команду:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   При вводе команды REPAIR STGPOOL поврежденные экстенты удаляются с тома сразу же после их исправления. Поврежденные экстенты не удерживаются в соответствии со значением, заданным в параметре REUSEDELAY.

3. Выявите все дополнительные поврежденные экстенты с помощью команды QUERY DAMAGED.
4. Если обнаружено повреждение, и дедуплицированные экстенты нельзя исправить с сервера репликации, все же остается возможность их исправления. В некоторых случаях клиентский узел повторно отправляет данные во время операции резервного копирования, и поврежденные экстенты исправляются. Подождите два цикла резервного копирования, чтобы разрешить операции резервного копирования на клиенте. После двух циклов резервного копирования выполните следующее:
   a. Чтобы убедиться, что повреждение исправлено, повторно введите команду QUERY DAMAGED.
   b. Если поврежден весь каталог пула хранения, создайте вместо него новый каталог пула хранения при помощи команды DEFINE STGPOOLDIRECTORY.
   c. Чтобы удалить объекты, ссылающиеся на поврежденные данные, введите команду AUDIT CONTAINER и задайте параметр ACTION=REMOVEDAMAGED.
      Например, чтобы выполнить аудит пула хранения каталога-контейнера с именем STGPOOL1, введите следующую команду:

      ```
      audit container stgpool=stgpool1 action=removedamaged
      ```

   d. Дополнительно, введите команду DELETE STGPOOLDIRECTORY, чтобы удалить пустой каталог пула хранения, который вы заменили на новый каталог на шаге 4.b.

Дальнейшие действия

Если в дальнейшем вы продолжаете обнаруживать поврежденные данные, введите команду AUDIT CONTAINER для пула хранения каталогов-контейнеров, чтобы определить, насколько широко распространились повреждения. Например, для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

```
audit container stgpool=stgpool1
```

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации для каталога-контейнера)
DEFINE SCHEDULE (определение расписания выполнения административных команд)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения)
PROTECT STGPOOL (Защитить данные пула хранения)
REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)
DEFINE STGPOOLDIRECTORY (Задать каталог пула хранения)

Восстановление пулов хранения с томов пула хранения контейнеров-копий

Если файлы, каталоги или пулы хранения на исходном сервере повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на исходном сервере путем извлечения экстентов дедуплицированных данных из локальных или удаленных ленточных томов пулов хранения контейнеров-копий.

Прежде чем начать

Сделайте следующее:

1. Оцените свою среду хранения и решите, что происходит в результате отключений питания, сетевых проблем и отказов оборудования: данные повреждаются или данные выглядят поврежденными. Если проблемы в вашей среде приводят к повреждению данных, найдите и исправьте эти проблемы.
2. Убедитесь, что в пуле хранения каталогов-контейнеров достаточно доступного пространства для восстановленных данных. Параметр PREVIEW=YES в команде REPAIR STGPOOL задает объем данных, которые будут исправлены. Если места недостаточно, воспользуйтесь командой DEFINE STGPOOLDIRECTORY для выделения пространства.
3. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
4. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
5. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
     b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
     c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить повреждения следующих типов:

- Незначительные повреждения, вызванные случайным удалением файлов или каталогов, перезаписью файлов, случайным изменением разрешений для файла или ошибками диска в связи с аппаратными проблемами.
- Умеренные повреждения, вызванные ошибками диска или ошибками монтирования диска. Такое повреждение приводит к потере одного или нескольких каталогов, но не к потере всего пула хранения.

Поврежденные дедуплицированные экстенты восстанавливаются по экстентам, которые были защищены в пулах хранения контейнеров-копий.
Ограничение: Команду REPAIR STGPOOL для заданного пула хранения можно ввести, только если вы уже скопировали данные в пулы хранения контейнеров-копий при помощи команды PROTECT STGPOOL.

При исправлении пула хранения каталога-контейнера их пулов контейнеров копий команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Пул хранения контейнера-копии недоступен.
- Пул хранения контейнера-копии поврежден.
- Тома пула хранения контейнера-копии недоступны или повреждены.

Процедура

1. Если вы подозреваете небольшое повреждение, введите команду AUDIT CONTAINER для пула хранения контейнеров на уровне каталога, чтобы выявить несогласованности между базой данных и пулом хранения каталогов-контейнеров. Выявив поврежденные экстенты данных в пуле хранения каталогов-контейнеров, вы сможете определить, какие экстенты данных следует исправить. Для сбережения времени и ресурсов выполняйте аудит только для контейнеров с подозрениями на повреждения. Если вы предполагаете, что ваш пул хранения контейнеров имеет более серьезные повреждения, введите команду AUDIT CONTAINER на уровне пула хранения. Например, для выполнения аудита каталога n:\pooldir в пуле хранения с именем STGPOOL1 введите команду:

   ```
   audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
   ```

   Для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

   ```
   audit container stgpool=stgpool1
   ```

   Процесс аудита может выполняться несколько часов.

   В ходе операции исправления сервер попросит вас указать тома, которые требуется исправить. На шаге 3 вы переносите тома в локальное положение и зарегистрируете их в библиотеке. Требуемые тома необходимо перенести в локальное положение и зарегистрировать в библиотеке.

2. Для предварительного просмотра операции исправления и генерирования списка ленточных томов, которые требуют ее выполнения, введите команду REPAIR STGPOOL и задайте параметры SRCLOCATION=LOCAL и PREVIEW=YES.
   Например, для предварительного просмотра операции исправления пула хранения с именем STGPOOL1 из пулов хранения контейнеров-копий введите команду:

   ```
   repair stgpool stgpool1 srclocation=local preview=yes
   ```

   Для выполнения предварительного просмотра может потребоваться некоторое время.

3. Если некоторые из нужных томов являются дистанционными, выполните следующие действия:
   a. Определите с помощью списка из операции предпросмотра, какие тома нужно перенести в локальное положение.
   b. Когда тома будут возвращены в локальное положение, зарегистрируйте их в библиотеке с помощью команды CHECKIN LIBVOLUME с параметром STATUS=PRIVATE.
   c. Обновите состояние томов с помощью команды UPDATE STGPOOL с параметром ACCESS=READWRITE.

   Подробные инструкции по функции менеджера аварийного восстановления (disaster recovery manager, DRM) смотрите в разделе Использование менеджера аварийного восстановления для ленточных сред (V7.1.1).
4. Используя информацию, полученную вами при выполнении операции предварительного просмотра, убедитесь, что в пуле хранения достаточно пространства для восстановленных данных. Если места недостаточно, воспользуйтесь командой DEFINE STGPOOLDIRECTORY для выделения пространства.
5. Для исправления пула хранения каталогов-контейнеров введите команду REPAIR STGPOOL и задайте параметр SRCLOCATION=LOCAL.
   Например, для исправления пула хранения с именем STGPOOL1 из пула хранения контейнеров-копий введите команду:

   ```
   repair stgpool stgpool1 srclocation=local
   ```

   При вводе команды REPAIR STGPOOL поврежденные экстенты удаляются с тома сразу же после их исправления. Поврежденные экстенты не удерживаются в соответствии со значением, заданным в параметре REUSEDELAY.

6. Выявите все дополнительные поврежденные экстенты с помощью команды QUERY DAMAGED.
7. Если обнаружено повреждение, и дедуплицированные экстенты нельзя исправить из пулов хранения контейнеров-копий, все же остается возможность их исправления. В некоторых случаях клиентский узел повторно отправляет данные во время операции резервного копирования, и поврежденные экстенты исправляются. Подождите два цикла резервного копирования, чтобы разрешить операции резервного копирования на клиенте. После двух циклов резервного копирования выполните следующее:

a. Чтобы убедиться, что повреждение исправлено, повторно введите команду QUERY DAMAGED.
b. Если поврежден весь каталог пула хранения, создайте вместо него новый каталог пула хранения при помощи команды DEFINE STGPOOLDIRECTORY.
c. Чтобы удалить объекты, ссылающиеся на поврежденные данные, введите команду AUDIT CONTAINER и задайте параметр ACTION=REMOVEDAMAGED.
Например, чтобы выполнить аудит пула хранения каталога-контейнера с именем STGPOOL1, введите следующую команду:

```
audit container stgpool=stgpool1 action=removedamaged
```

d. Дополнительно, введите команду DELETE STGPOOLDIRECTORY, чтобы удалить пустой каталог пула хранения, который вы заменили на новый каталог на шаге 7.b.

8. Если исправления коснулись всего каталога пула хранения, удалите исходный каталог, который пуст и заменен новым каталогом. Для удаления исходного каталога введите команду DELETE STGPOOLDIRECTORY.

Дальнейшие действия

Если в дальнейшем вы продолжаете обнаруживать поврежденные данные, введите команду AUDIT CONTAINER для пула хранения каталогов-контейнеров, чтобы определить, насколько широко распространились повреждения. Например, для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

```
audit container stgpool=stgpool1
```

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации для каталога-контейнера)
DEFINE SCHEDULE (определение расписания выполнения административных команд)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения)
PROTECT STGPOOL (Защитить данные пула хранения)
REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)
DEFINE STGPOOLDIRECTORY (Задать каталог пула хранения)
DELETE STGPOOLDIRECTORY (Удалить каталог пула хранения)

Исправление пулов хранения в среде с сервером репликации и томами пула хранения контейнеров-копий

Если файлы, каталоги или пулы хранения на исходном сервере повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на исходном сервере репликации путем извлечения экстентов дедуплицированных данных с сервера репликации назначения или из ленточных томов пулов хранения контейнеров-копий.

Прежде чем начать

Сделайте следующее:

1. Оцените свою среду хранения и решите, что происходит в результате отключений питания, сетевых проблем и отказов оборудования: данные повреждаются или данные выглядят поврежденными. Если проблемы в вашей среде приводят к повреждению данных, найдите и исправьте эти проблемы.
2. Убедитесь, что в пуле хранения каталогов-контейнеров достаточно доступного пространства для восстановленных данных. Параметр PREVIEW=YES в команде REPAIR STGPOOL задает объем данных, которые будут исправлены. Если места недостаточно, воспользуйтесь командой DEFINE STGPOOLDIRECTORY для выделения пространства.
3. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
4. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
5. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или

дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:

a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.

- Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
  a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
  b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
  c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить повреждения следующих типов:

- Незначительные повреждения, вызванные случайным удалением файлов или каталогов, перезаписью файлов, случайным изменением разрешений для файла или ошибками диска в связи с аппаратными проблемами.
- Умеренные повреждения, вызванные ошибками диска или ошибками монтирования диска. Такое повреждение приводит к потере одного или нескольких каталогов, но не к потере всего пула хранения.

Поврежденные дедуплицированные экстенты восстанавливаются по экстентам, которые были защищены на сервере репликации назначения или в пулах хранения контейнеров-копий на исходном сервере.
Ограничение: Команду REPAIR STGPOOL для заданного пула хранения можно ввести, только если вы уже скопировали данные в другой пул хранения на сервере репликации назначения или в пулы хранения контейнеров-копий при помощи команды PROTECT STGPOOL.
При исправлении пула хранения каталога-контейнера с целевого сервера репликации команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Целевой сервер репликации недоступен.
- Целевой пул хранения поврежден.
- Произошло отключение сети.

При исправлении пула хранения каталога-контейнера их пулов контейнеров копий команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Пул хранения контейнера-копии недоступен.
- Пул хранения контейнера-копии поврежден.
- Тома пула хранения контейнера-копии недоступны или повреждены.

Процедура

1. Попытка исправить пул хранения с сервера репликации назначения с выполнением действий, описанных в разделе Восстановление пулов хранения с целевого сервера репликации.
2. Если поврежденные экстенты нельзя исправить с сервера репликации назначения, восстановите их из внешних пулов хранения контейнеров-копий, выполнив действия из раздела Восстановление пулов хранения с томов пула хранения контейнеров-копий.
3. Если вы восстановили поврежденные экстенты из пулов хранения контейнеров-копий, введите команду PROTECT STGPOOL и задайте параметр TYPE=REPLSERVER для пулов хранения на исходном сервере репликации.

Дальнейшие действия

Если в дальнейшем вы продолжаете обнаруживать поврежденные данные, введите команду AUDIT CONTAINER для пула хранения каталогов-контейнеров, чтобы определить, насколько широко распространились повреждения. Например, для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

```
audit container stgpool=stgpool1
```

Ссылки, связанные с данной:

AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации для каталога-контейнера)
DEFINE SCHEDULE (определение расписания выполнения административных команд)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения)
PROTECT STGPOOL (Защитить данные пула хранения)
REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)
DEFINE STGPOOLDIRECTORY (Задать каталог пула хранения)
DELETE STGPOOLDIRECTORY (Удалить каталог пула хранения)

Исправление пулов хранения на сервере репликации назначения

Если файлы, каталоги или пулы хранения на сервере репликации назначения повреждены, можно исправить экстенты данных в пуле хранения каталогов-контейнеров на сервере репликации назначения путем извлечения экстентов дедуплицированных данных с исходного сервера репликации.

Прежде чем начать

Сделайте следующее:

1. Оцените свою среду хранения и решите, что происходит в результате отключений питания, сетевых проблем и отказов оборудования: данные повреждаются или данные выглядят поврежденными. Если проблемы в вашей среде приводят к повреждению данных, найдите и исправьте эти проблемы.
2. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
3. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
4. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
     b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
     c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить повреждения следующих типов:

- Незначительные повреждения, вызванные случайным удалением файлов или каталогов, перезаписью файлов, случайным изменением разрешений для файла или ошибками диска в связи с аппаратными проблемами.
- Умеренные повреждения, вызванные ошибками диска или ошибками монтирования диска. Такое повреждение приводит к потере одного или нескольких каталогов, но не к потере всего пула хранения.

В процессе операции по выполнению команды PROTECT STGPOOL исправляются поврежденные экстенты в пуле хранения назначения. Чтобы исправить экстенты, они должны уже быть отмечены на сервере назначения как поврежденные.

Например, команда AUDIT CONTAINER может выявить повреждение в пуле хранения назначения до ввода команды PROTECT STGPOOL.

Процедура

1. Защитите экстенты данных в пуле хранения каталогов-контейнеров на исходном сервере с помощью команды PROTECT STGPOOL.
   Например, чтобы защитить пул хранения каталога-контейнера с именем POOL1, введите следующую команду:

   ```
   protect stgpool pool1
   ```

   Дождитесь завершения процесса защиты.

2. Чтобы выявить поврежденные экстенты данных в пуле хранения каталогов-контейнеров на сервере назначения, введите команду AUDIT CONTAINER.
   Например, для выполнения аудита пула хранения с именем STGPOOL1 дайте следующую команду:

   ```
   audit container stgpool=stgpool1
   ```

3. Исправьте поврежденные экстенты в пуле хранения назначения, повторно введя команду PROTECT STGPOOL на исходном сервере. Поврежденные экстенты в пуле хранения назначения будут помечены как поврежденные и исправлены.
4. Убедитесь, что больше нет поврежденных экстентов, для чего введите команду QUERY DAMAGED.

Ссылки, связанные с данной:
AUDIT CONTAINER (Проверка непротиворечивости содержащейся в базе данных информации для каталога-контейнера)
DEFINE SCHEDULE (определение расписания выполнения административных команд)
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения)
PROTECT STGPOOL (Защитить данные пула хранения)
REPAIR STGPOOL (Восстановить пул хранения каталога-контейнера)
DEFINE STGPOOLDIRECTORY (Задать каталог пула хранения)
DELETE STGPOOLDIRECTORY (Удалить каталог пула хранения)

Восстановление пулов хранения после аварии

Можно восстановить пулы хранения каталогов-контейнеров и возвратить их потерянные данные после аварии.

В случае аварии, если ваш основной узел более недоступен, можно исправить пулы хранения каталогов-контейнеров, восстановив их на новом сервере назначения на узле восстановления.

- Восстановление пулов хранения с томов пула хранения контейнеров-копий после аварии
  Если авария произошла на исходном сервере, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с внешних ленточных томов пула хранения контейнеров-копий. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.
- Исправление пулов хранения с сервера репликации назначения после аварии
  Если авария произошла на исходном сервере репликации, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с сервера репликации назначения. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.
- Исправление пулов хранения в среде с сервером репликации и томами пула хранения контейнеров-копий после аварии
  Если авария произошла на исходном сервере, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с сервера репликации назначения или с внешних ленточных томов пула хранения контейнеров-копий. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.

Ссылки, связанные с данной:
Как указать, следует ли использовать пулы хранения контейнеров для защиты при авариях

Восстановление пулов хранения с томов пула хранения контейнеров-копий после аварии

Если авария произошла на исходном сервере, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с внешних ленточных томов пула хранения контейнеров-копий. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.

Прежде чем начать

Сделайте следующее:

1. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
2. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
3. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
     b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
     c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить крупные повреждения следующих типов:

- Полная потеря всех пулов хранения контейнеров на исходном сервере
- Полная потеря основного узла

Для этого сценария аварийного восстановления сделаны следующие допущения:

- Вы использовали команду PROTECT STGPOOL для резервного копирования данных во внешние пулы хранения контейнеров-копий с исходного сервера. Вы извлекли внешние ленточные тома и разместили их на своем узле восстановления.
- Вы не использовали команду PROTECT STGPOOL для резервного копирования данных на сервер репликации назначения.
- Вы использовали макеты IBM Spectrum Protect Blueprint для конфигурирования исходного сервера IBM Spectrum Protect, а также сценарии конфигурирования макетов для восстановления среды путем конфигурирования нового сервера назначения на узле восстановления. В этих сценариях резервные копии базы данных IBM Spectrum Protect, файла серверных опций (dsmserv.opt), файла хронологии томов (volhist.out) и файла конфигурации устройств (devconfig.out) копируются в их исходные положения на сервере восстановления. После запуска этих сценариев вы увидите на сервере восстановления вновь созданные пустые каталоги.

При попытке исправления пула хранения каталога-контейнера их пулов контейнеров копий команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Пул хранения контейнера-копии недоступен.
- Пул хранения контейнера-копии поврежден.

- Тома пула хранения контейнера-копии недоступны или повреждены.

Процедура

1. Пометьте все экстенты данных в пуле хранения контейнеров как поврежденные с помощью команды AUDIT CONTAINER для пула хранения контейнеров на уровне пула хранения, задав параметр ACTION=MARKDAMAGED. Например, чтобы выполнить аудит пула хранения с именем STGPOOL1 и пометить его как поврежденный, введите следующую команду:

   ```
   audit container stgpool=stgpool1 action=markdamaged
   ```

2. Если вы использовали для защиты пула хранения каталогов-контейнеров как локальные, так и внешние пулы хранения контейнеров-копий, введите команду UPDATE STGPOOL для локальной копии пулов хранения контейнеров-копий и задайте параметр ACCESS=UNAVAILABLE.
3. Когда тома внешнего пула хранения контейнеров-копий будут возвращены в локальное положение, зарегистрируйте их в библиотеке с помощью команды CHECKIN LIBVOLUMEc с параметром STATUS=PRIVATE.
4. Обновите состояние томов с помощью команды UPDATE STGPOOL с параметром ACCESS=READWRITE.
5. Исправьте пул хранения с помощью команды REPAIR STGPOOL с параметром SRCLOCATION=LOCAL. Например, для исправления пула хранения с именем STGPOOL1 из внешнего пула хранения контейнеров-копий введите команду:

   ```
   repair stgpool stgpool1 srclocation=local
   ```

   При вводе команды REPAIR STGPOOL поврежденные экстенты удаляются с тома сразу же после их исправления. Поврежденные экстенты не удерживаются в соответствии со значением, заданным в параметре REUSEDELAY.

6. Убедитесь, что больше нет поврежденных экстентов, для чего введите команду QUERY DAMAGED.
7. Повторите эту процедуру для исправления всех пулов хранения.

Исправление пулов хранения с сервера репликации назначения после аварии

Если авария произошла на исходном сервере репликации, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с сервера репликации назначения. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.

Прежде чем начать

Сделайте следующее:

1. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
2. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
3. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:

a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить крупные повреждения следующих типов:

- Полная потеря всех пулов хранения контейнеров на исходном сервере репликации
- Полная потеря основного узла

Для этого сценария аварийного восстановления сделаны следующие допущения:

- Вы использовали команду PROTECT STGPOOL для резервного копирования данных с исходного сервера репликации на сервер репликации назначения. Сервер репликации назначения запущен на вашем узле восстановления.
- Вы не использовали команду PROTECT STGPOOL для резервного копирования данных во внешние пулы хранения контейнеров-копий.
- Вы использовали макеты IBM Spectrum Protect Blueprint для конфигурирования исходного сервера IBM Spectrum Protect, а также сценарии конфигурирования макетов для восстановления среды путем конфигурирования нового сервера назначения на узле восстановления. В этих сценариях резервные копии базы данных IBM Spectrum Protect, файла серверных опций (dsmserv.opt), файла хронологии томов (volhist.out) и файла конфигурации устройств (devconfig.out) копируются в их исходные положения на сервере восстановления. После запуска этих сценариев вы увидите на сервере восстановления вновь созданные пустые каталоги.

При попытке исправления пула хранения каталога-контейнера с целевого сервера репликации команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Целевой сервер репликации недоступен.
- Целевой пул хранения поврежден.
- Произошло отключение сети.

Процедура

1. Пометьте все экстенты данных в пуле хранения контейнеров как поврежденные с помощью команды AUDIT CONTAINER для пула хранения контейнеров на уровне пула хранения, задав параметр ACTION=MARKDAMAGED. Например, чтобы выполнить аудит пула хранения с именем STGPOOL1 и пометить его как поврежденный, введите следующую команду:

   ```
   audit container stgpool=stgpool1 action=markdamaged
   ```

2. Исправьте пул хранения с помощью команды REPAIR STGPOOL с параметром SRCLOCATION=REPLSERVER. Например, для исправления пула хранения с именем STGPOOL1 с сервера репликации назначения введите команду:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   При вводе команды REPAIR STGPOOL поврежденные экстенты удаляются с тома сразу же после их исправления. Поврежденные экстенты не удерживаются в соответствии со значением, заданным в параметре REUSEDELAY.

3. Если вы не использовали сценарии конфигурирования Blueprint для настройки вашего сервера репликации назначения, структура файлов на сервере репликации назначения может не соответствовать информации, хранящейся в базе данных. Дополнительно можно удалить каталоги пула хранения, которые не существуют на сервере репликации назначения с помощью команды DELETE STGPOOLDIRECTORY.
4. Убедитесь, что больше нет поврежденных экстентов, для чего введите команду QUERY DAMAGED.
5. Если обнаружено повреждение, и дедуплицированные экстенты нельзя исправить с сервера репликации, все же остается возможность их исправления. В некоторых случаях клиентский узел повторно отправляет данные во время операции резервного копирования, и поврежденные экстенты исправляются. Подождите два цикла резервного копирования, чтобы разрешить операции резервного копирования на клиенте. После двух резервного копирования выполните следующее:
   a. Чтобы убедиться, что повреждение исправлено, повторно введите команду QUERY DAMAGED.

b. Чтобы удалить объекты, ссылающиеся на поврежденные данные, введите команду AUDIT CONTAINER и задайте параметр ACTION=REMOVEDAMAGED.
Например, чтобы выполнить аудит пула хранения каталога-контейнера с именем STGPOOL1, введите следующую команду:

```
audit container stgpool=stgpool1 action=removedamaged
```

6. Повторите эту процедуру для исправления всех пулов хранения.

Ссылки, связанные с данной:
QUERY DAMAGED (Запросить поврежденные данные в пуле хранения)

Исправление пулов хранения в среде с сервером репликации и томами пула хранения контейнеров-копий после аварии

Если авария произошла на исходном сервере, можно исправить экстенты дедуплицированных данных в пуле хранения каталогов-контейнеров с сервера репликации назначения или с внешних ленточных томов пула хранения контейнеров-копий. Для пула хранения каталогов-контейнеров исправления выполняются на сервере назначения на узле восстановления.

Прежде чем начать

Выполните следующие задачи:

1. Создайте резервную копию базы данных сервера IBM Spectrum Protect, используя один из следующих методов:
   - На странице Обзоры в компоненте Центр операций щелкните по Серверы, выберите сервер и щелкните по Создать резервную копию.
   - Введите команду администрирования BACKUP DB.
2. Ознакомьтесь с последней информацией об исправлении и восстановлении данных в техническом замечании 2013682.
3. Чтобы спланировать следующие шаги, прочтите о следующих ограничениях при использования команды AUDIT CONTAINER:
   Внимание:
   - Если ввести команду AUDIT CONTAINER с параметром ACTION=MARKDAMAGED для всего пула хранения, данные, на которые есть ссылки, будут недоступны для операций восстановления, пока пул хранения не будет исправлен. В зависимости от размера базы данных, сетевой ширины полосы пропускания, скорости носителя и других факторов команда REPAIR STGPOOL может выполняться в течение нескольких часов или дней. Поэтому, если какие-то данные в пуле хранения доступны или если состояние данных в пуле хранения неизвестно, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду AUDIT CONTAINER с параметром ACTION=SCANALL. Параметр ACTION=SCANALL указывает записи базы данных, ссылающиеся на экстенты данных с противоречиями. Только такие экстенты данных будут помечены в базе данных как поврежденные.
     b. После того как экстенты будут помечены как поврежденные, можно выполнить команду REPAIR STGPOOL.
   - Если вы собираетесь ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAMAGED, следуйте приведенным ниже рекомендациям:
     a. Рассмотрите возможность сначала ввести команду QUERY DAMAGED, чтобы определить область поврежденных экстентов данных в пуле хранения.
     b. После этого можно ввести команду REPAIR STGPOOL, чтобы восстановить поврежденные экстенты в пуле хранения.
     c. И, наконец, можно ввести команду AUDIT CONTAINER с параметром ACTION=REMOVEDAAMAGED, чтобы удалить все поврежденные экстенты данных, оставшиеся в пуле хранения.

Об этой задаче

С помощью этой процедуры можно исправить крупные повреждения следующих типов:

- Полная потеря всех пулов хранения контейнеров на исходном сервере
- Полная потеря основного узла

Для этого сценария аварийного восстановления сделаны следующие допущения:

- Вы использовали команду PROTECT STGPOOL для резервного копирования данных с исходного сервера репликации на сервер репликации назначения. Сервер репликации назначения запущен на вашем узле восстановления.
- Вы использовали команду PROTECT STGPOOL для резервного копирования данных во внешние пулы хранения контейнеров-копий.
- Вы использовали макеты IBM Spectrum Protect Blueprint для конфигурирования исходного сервера IBM Spectrum Protect, а также сценарии конфигурирования макетов для восстановления среды путем конфигурирования нового сервера назначения на узле восстановления. В этих сценариях резервные копии базы данных IBM Spectrum Protect, файла серверных опций (dsmserv.opt), файла хронологии томов (volhist.out) и файла конфигурации устройств (devconfig.out) копируются в их исходные положения на сервере восстановления. После запуска этих сценариев вы увидите на сервере восстановления вновь созданные пустые каталоги.

При попытке исправления пула хранения каталога-контейнера с целевого сервера репликации команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Целевой сервер репликации недоступен.
- Целевой пул хранения поврежден.
- Произошло отключение сети.

При исправлении пула хранения каталога-контейнера их пулов контейнеров копий команда REPAIR STGPOOL завершится неудачно, если будет выполнено любое из следующих условий:

- Пул хранения контейнера-копии недоступен.
- Пул хранения контейнера-копии поврежден.
- Тома пула хранения контейнера-копии недоступны или повреждены.

Процедура

1. Пометьте все экстенты данных в пуле хранения контейнеров как поврежденные с помощью команды AUDIT CONTAINER для пула хранения контейнеров на уровне пула хранения, задав параметр ACTION=MARKDAMAGED. Например, чтобы выполнить аудит пула хранения с именем STGPOOL1 и пометить его как поврежденный, введите следующую команду:

   ```
   audit container stgpool=stgpool1 action=markdamaged
   ```

2. Если вы использовали для защиты пула хранения каталогов-контейнеров как локальные, так и внешние пулы хранения контейнеров-копий, введите команду UPDATE STGPOOL для локальной копии пулов хранения контейнеров-копий и задайте параметр ACCESS=UNAVAILABLE.
3. Когда тома внешнего пула хранения контейнеров-копий будут возвращены в локальное положение, зарегистрируйте их в библиотеке с помощью команды CHECKIN LIBVOLUMEс с параметром STATUS=PRIVATE. Перемещая ленточные тома в локальное положение сейчас, вы создаете условия для исправления поврежденных экстентов из ленточных томов контейнеров-копий, если эти экстенты нельзя исправить с сервера репликации назначения.
4. Обновите состояние томов с помощью команды UPDATE STGPOOL с параметром ACCESS=READWRITE.
5. Исправьте пул хранения с помощью команды REPAIR STGPOOL с параметром SRCLOCATION=REPLSERVER. Например, для исправления пула хранения с именем STGPOOL1 с сервера репликации назначения введите команду:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   При вводе команды REPAIR STGPOOL поврежденные экстенты удаляются с тома сразу же после их исправления. Поврежденные экстенты не удерживаются в соответствии со значением, заданным в параметре REUSEDELAY.

6. Если вы не использовали сценарии конфигурирования Blueprint для настройки вашего сервера репликации назначения, структура файлов на сервере репликации назначения может не соответствовать информации, хранящейся в базе данных. Дополнительно можно удалить каталоги пула хранения, которые не существуют на сервере репликации назначения. Введите команду DELETE STGPOOLDIRECTORY, чтобы удалить каталоги, отсутствующие на сервере репликации назначения.
7. Убедитесь, что больше нет поврежденных экстентов, для чего введите команду QUERY DAMAGED.
8. Если поврежденные экстенты нельзя исправить с сервера репликации назначения, их можно исправить из внешних пулов хранения контейнеров-копий. Инструкции смотрите в разделе Восстановление пулов хранения с томов пула хранения контейнеров-копий после аварии.
9. Убедитесь, что больше нет поврежденных экстентов, для чего повторно введите команду QUERY DAMAGED.

10. Если обнаружено повреждение, и дедуплицированные экстенты нельзя исправить с сервера репликации, все же остается возможность их исправления. В некоторых случаях клиентский узел повторно отправляет данные во время операции резервного копирования, и поврежденные экстенты исправляются. Подождите два цикла резервного копирования, чтобы разрешить операции резервного копирования на клиенте. После двух циклов резервного копирования выполните следующее:
    a. Чтобы убедиться, что повреждение исправлено, повторно введите команду QUERY DAMAGED.
    b. Чтобы удалить объекты, ссылающиеся на поврежденные данные, введите команду AUDIT CONTAINER и задайте параметр ACTION=REMOVEDAMAGED.
    Например, чтобы выполнить аудит пула хранения каталога-контейнера с именем STGPOOL1, введите следующую команду:

    ```
    audit container stgpool=stgpool1 action=removedamaged
    ```

11. Повторите эту процедуру для исправления всех пулов хранения.

Замена поврежденного ленточного тома пула хранения контейнеров-копий

Если ленточный том, в котором хранятся копии дедуплицированных экстентов данных пула хранения контейнеров-копий, поврежден, можно заменить этот том.

Процедура

1. Удалите поврежденный ленточный том с помощью команды DELETE VOLUME с параметром DISCARDDATA=YES.
   Например, для удаления тома с именем VOLUME1 дайте следующую команду:

   ```
   delete volume volume1 discarddata=yes
   ```

2. Защитите экстенты данных в пуле хранения каталогов-контейнеров, скопировав данные в существующие тома в пуле хранения контейнеров-копий. Введите команду PROTECT STGPOOL с исходного сервера.
   Например, чтобы защитить пул хранения каталога-контейнера с именем POOL1, введите следующую команду:

   ```
   protect stgpool pool1 type=local
   ```

Ссылки, связанные с данной:
PROTECT STGPOOL (Защитить данные пула хранения)
DELETE VOLUME (удаление тома пула хранения)

Server commands, options, and utilities

Use commands to administer and configure the server, options to customize the server, and utilities to perform special tasks when the server is not running.

- Managing the server from the command line
  IBM Spectrum Protect™ provides several different command-line interfaces for managing IBM Spectrum Protect servers.
- Administrative commands
  Administrative commands are available to manage and configure the server.
- Server options
  At installation, IBM Spectrum Protect provides a server options file that contains a set of default options to start the server.
- Server utilities
  Use server utilities to perform special tasks on the server while the server is not running.
- Return codes for use in IBM Spectrum Protect scripts
  You can write IBM Spectrum Protect scripts that use return codes to determine how script processing proceeds. The return codes can be one of three severities: OK, WARNING, ERROR.
- Device utilities
  You can use device utilities for tasks that are related to configuring storage devices for the IBM Spectrum Protect server.
- Server scripts and macros for automation
  You can automate common administrative tasks by creating IBM Spectrum Protect server scripts or administrative client macros. Server scripts are stored in the server database and can be scheduled to run with an administrative schedule command. Administrative client macros are stored as files on the administrative client.

Managing the server from the command line

IBM Spectrum Protect™ provides several different command-line interfaces for managing IBM Spectrum Protect servers.

About this task

The following command-line interfaces are available:

Administrative command-line client
: The administrative command-line client is a program that runs on a file server, workstation, or mainframe. It is installed as part of the IBM Spectrum Protect server installation process. The administrative client can be accessed remotely.

  From the administrative client, you can issue any server commands.

Server console
: The server console is a command-line window on the system where the server is installed. Therefore, to use the server console, you must be at the physical location of the server system.

  Compared to the administrative client, the capabilities of the server console are limited. From the server console, you cannot issue certain commands, and you cannot route commands to other servers. Also, you cannot specify that certain commands process before other commands can be issued. However, this limitation can be useful if, for example, you want to run two commands in quick succession.

Operations Center command line
: From the Operations Center, you can access the IBM Spectrum Protect command line. You might want to use this command line to issue server commands to complete certain IBM Spectrum Protect tasks that are not supported in the Operations Center.

Server scripts provide for automation of common administrative tasks. A macro is a file that contains one or more IBM Spectrum Protect administrative commands. When you issue the MACRO command, the server processes all commands in the macro file in order, including commands that are contained in any nested macros.

- Issuing commands from the administrative client
  The administrative command-line client is a program that runs on a file server, workstation, or mainframe.
- Issuing commands from the Operations Center
  From the Operations Center command-line interface, you can issue commands to manage IBM Spectrum Protect servers that are configured as hub or spoke servers.
- Issuing commands from the server console
  IBM Spectrum Protect provides a user ID named SERVER_CONSOLE that allows you to issue commands and administer the server from the server console after IBM Spectrum Protect is installed. At installation, SERVER_CONSOLE is automatically registered as an administrator and is given system authority.
- Entering administrative commands
  Commands consist of command names and usually parameters and variables. Syntax diagrams depict the rules to follow when entering commands.
- Controlling command processing
  You can run some IBM Spectrum Protect commands sequentially or concurrently with other commands. You can also route commands from one server to other servers for processing.
- Performing tasks concurrently on multiple servers
  Command routing allows you to route commands to one or more servers for processing and then collect the output from these servers.
- Privilege classes for commands
  The authority granted to an administrator through the privilege class determines which administrative commands that the administrator can issue.

Related concepts:
Server scripts
Related reference:
Administrative client macros

Issuing commands from the administrative client

The administrative command-line client is a program that runs on a file server, workstation, or mainframe.

About this task

Ensure that your administrative client and your server are running in compatible languages. See LANGUAGE for language and locale options. If your client and server are using different languages, the messages that IBM Spectrum Protect™ generates might not be understandable.

Tip: Text strings that are sent from the client to the server do not depend on the server language setting. The text is displayed properly if the administrative client runs in the same locale when sending the string and when receiving the string.

For example, assume that you update a node contact field with a value that contains national characters (`update node myNode contact=NLcontact_info`), and later query the node (`query node myNode format=detailed`). If the client is running in the same locale when you update as when you query, the *NLcontact_info* displays properly. If you update the node contact field when the client is running in one locale, and query the node when the client is running in a different locale, the *NLcontact_info* might not display properly.

- Starting and stopping the administrative client
  Use the DSMADMC command to start an administrative client session.
- Monitoring server activities from the administrative client
  To monitor IBM Spectrum Protect activities, such as server migration and client logons, run the administrative client in console mode. You cannot enter any administrative commands in console mode.
- Monitoring removable-media mounts from the administrative client
  To monitor the mounting and dismounting of removable media, run the administrative client in mount mode. When the client is running in mount mode, you cannot enter any administrative commands.
- Processing individual commands from the administrative client
  Use batch mode to enter a single administrative command. Your administrative client session automatically ends when the command is processed.
- Processing a series of commands from the administrative client
  Use the interactive mode to process a series of administrative commands.
- Formatting output from commands
  IBM Spectrum Protect formats the output processed from commands according to your screen or window width.
- Saving command output to a specified location
  The most common use for redirecting output is to save the output from query commands to a specified file or program. You can then browse the contents of the file or in some cases, print the contents.
- Administrative client options
  In all administrative client modes, you can use options to modify administrative client session responses.

Starting and stopping the administrative client

Use the DSMADMC command to start an administrative client session.

About this task

The IBM Spectrum Protect™ server must be running before an administrative client can connect.

Procedure

- To start an administrative client session in command-line mode, enter this command on your workstation:

  ```
  dsmadmc -id=admin -password=adminpwd -dataonly=yes
  ```

  By entering the DSMADMC command with the -ID and -PASSWORD options as shown, you are not prompted for a user ID and password.

- To stop an administrative command-line client session, enter the following command:

  ```
  quit
  ```

- To interrupt a DSMADMC command before the IBM Spectrum Protect server finishes processing it, use the UNIX `kill -9` command from an available command line. Do not press `Ctrl+C` because, while it ends the session, it can lead to unexpected results.

Monitoring server activities from the administrative client

To monitor IBM Spectrum Protect™ activities, such as server migration and client logons, run the administrative client in console mode. You cannot enter any administrative commands in console mode.

Procedure

- To start an administrative client session in console mode, enter the following command:

  ```
  dsmadmc -consolemode
  ```

  You are prompted for a password if authentication is turned on for the server. If you do not want to be prompted for your user ID and password, enter the DSMADMC command with the -ID and -PASSWORD options.

- To end an administrative client session in console mode, use a keyboard break sequence.

Operating system	Break sequence
UNIX and Linux clients	Ctrl+C
Windows clients	Ctrl+C or Ctrl+Break

Monitoring removable-media mounts from the administrative client

To monitor the mounting and dismounting of removable media, run the administrative client in mount mode. When the client is running in mount mode, you cannot enter any administrative commands.

Procedure

- To start an administrative client session in mount mode, enter the following command:

  ```
  dsmadmc -mountmode
  ```

  You are prompted for a password if authentication is turned on for the server. If you do not want to be prompted for your user ID and password, enter the DSMADMC command with the -ID and -PASSWORD options.

- To end an administrative client session in mount mode, use a keyboard break sequence.

Operating system	Break sequence
UNIX and Linux clients	Ctrl+C
Windows clients	Ctrl+C or Ctrl+Break

Processing individual commands from the administrative client

Use batch mode to enter a single administrative command. Your administrative client session automatically ends when the command is processed.

Procedure

To start an administrative client session in batch mode, use the following command: `dsmadmc server_command`

If you do not want to be prompted for your user ID and password, you can enter the DSMADMC command with the -ID and -PASSWORD options.

In batch mode, you must enter the complete command on one line. If a command does not fit on one line, enter the command by using a macro or a script. If you specify a parameter with a string of text using batch mode, enclose the text in single quotation marks (' ') in the macro. Do not use double quotation marks for commands in batch mode, because your operating system might not parse the quotation marks correctly.

Windows You can bypass this batch mode double quotation mark restriction for Windows clients by using the back slash (\) escape character. For example, on the OBJECTS parameter of the DEFINE CLIENTACTION command, you could enter the string with the \ character preceding the double quotation marks in the command.

```
dsmadmc -id=admin -password=admin define clientaction test_node domain=test_dom
action=restore objects='\"C:\program files\test\*\"'
```

Processing a series of commands from the administrative client

Use the interactive mode to process a series of administrative commands.

About this task

To start an administrative client session in interactive mode, a server session must be available. To ensure the availability of server sessions for both administrative and client node sessions, the interactive mode of the administrative client is disconnected if one or more of the following conditions is true:

- The server was stopped by using the HALT command.
- Commands were not issued from the administrative client session for the length of time that is specified with the IDLETIMEOUT server option.
- The administrative client session was canceled with the CANCEL SESSION command.

Procedure

To start an administrative session in interactive mode, use the following command: `dsmadmc`

You can use continuation characters when you use interactive mode. For more information, see t_cmdline_longcmd.dita#t_cmdline_longcmd.

You can automatically restart your administrative client session by entering another command each time the `tsm: servername >` prompt appears.

Do not enter a server command with the DSMADMC command. Doing so starts the administrative client in batch, not interactive, mode. For example, do not enter:

```
dsmadmc server_command
```

Formatting output from commands

IBM Spectrum Protect™ formats the output processed from commands according to your screen or window width.

Procedure

- If the width of your screen or window is not wide enough to display the output horizontally, IBM Spectrum Protect arranges and displays the information vertically.
- You can format the output of QUERY commands using the DISPLAYMODE and OUTFILE administrative client options.

Saving command output to a specified location

The most common use for redirecting output is to save the output from query commands to a specified file or program. You can then browse the contents of the file or in some cases, print the contents.

About this task

On some operating systems, you can redirect output of a command by using special characters such as >, >>, and |. Redirection characters direct the output of a command to a file or program that you specify instead of to your screen. You can save the output from a command by entering redirection characters at the end of the command. To redirect output, leave a blank between the redirection character and the file or program name. See the following examples.

When redirecting output, follow the naming conventions of the operating system where you are running the administrative client.

Procedure

The examples in the following table show how to redirect command output.

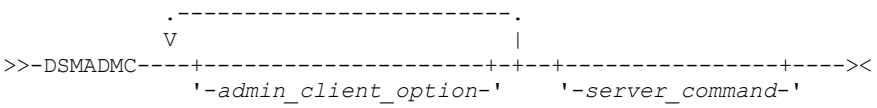
Task	Procedure

Task	Procedure
Redirect the output of a QUERY DOMAIN command to a new file in batch or interactive mode	Use a single greater-than sign (>) to redirect the output to a new file or write over an existing file: `dsmadmc -id=sullivan -pa=secretpwd query domain acctg > dominfo.acc`
Append the output of a QUERY DOMAIN command to the end of an existing file in batch or interactive mode	Use two consecutive greater-than signs (>>) to append the output to the end of an existing file: `dsmadmc -id=sullivan -pa=secretpwd query domain acctg >> dominfo.acc`
Redirect all output from an administrative client session in console mode to a program called filter.exe	Use the vertical bar (|) to direct all output for a session to a program: `dsmadmc -console -id=sullivan -password=secretpwd | filter.exe` The program can be set up to monitor the output for individual messages as they occur and take appropriate action, such as sending mail to another user.
In console mode, redirect all output to a file	Specify the -OUTFILE option with a destination file name. For example, the following command redirects all output to the save.out file: `dsmadmc -id=sullivan -password=secretpwd -consolemode -outfile=save.out`

Administrative client options

In all administrative client modes, you can use options to modify administrative client session responses.

Syntax



Example of using administrative client options

You can enter the DSMADMC command with your user ID and password by using the -ID and -PASSWORD options so that you are not prompted for that information. To have IBM Spectrum Protect™ redirect all output to a file, specify the -OUTFILE option with a destination file name. For example, to issue the QUERY NODE command in batch mode with the output redirected to the SAVE.OUT file, enter:

```
dsmadmc -id=sullivan -password=secret -outfile=save.out query node
```

Options

Administrative client options can be specified with the DSMADMC command and are valid from an administrative client session only. You can type an option in uppercase letters, lowercase letters, or any combination. Uppercase letters denote the shortest acceptable abbreviation. If an option appears entirely in uppercase letters, you cannot abbreviate it.

-ALWAYSPrompt
: Specifies that a command prompt is displayed if the input is from the keyboard or if it is redirected (for example, from a file). If this option is not specified and the input is redirected, the command prompt is not written.

  If the input is redirected, only the command output is displayed. If this option is specified, the command prompt and the command output are displayed.

-CHECKAliashalt
: Allows the administrative client to recognize an alias for the HALT command as set in the ALIASHALT server option. See ALIASHALT for details.

-COMMAdelimited

Specifies that any tabular output from a server query is to be formatted as comma-separated strings rather than in readable format. This option is intended to be used primarily when you redirect the output of an SQL query (SELECT command). The comma-separated value format is a standard data format, which can be processed by many common programs, including spreadsheets, databases, and report generators.

-CONsolemode

Specifies that IBM Spectrum Protect runs in console mode. Most server console output is echoed to your screen. The exception are items such as responses to query commands that are issued from the console, trace output, or any system messages that displayed on the console.

-DATAONLY=NO or YES

Specifies whether product version information and output headers display with the output. The default is NO.

NO

Specifies that the product version information and output column headers display.

YES

Suppresses the product version information and output column headers.

-DISPLaymode=LISt or TABle

You can force the QUERY output to tabular or list format regardless of the command-line window column width.

If you are using the -DISPLAYMODE option and you want the output to go to a file, do not specify the -OUTFILE option. Use redirection to write to the file.

-ID=userid

Specifies the administrator's user ID.

-Itemcommit

Specifies that IBM Spectrum Protect commits commands inside a script or a macro as each command is processed.

-MOUNTmode

Specifies that IBM Spectrum Protect runs in mount mode. All server removable-media mount messages are echoed to your screen.

-NEWLINEAFTERPrompt

Specifies that a newline character is written after the command prompt and commands that are entered from the keyboard are displayed underneath the prompt. If this option is not specified, commands entered from the keyboard are displayed to the right side of the prompt.

-NOConfirm

Specifies that you do not want IBM Spectrum Protect to request confirmation before processing commands that affect the availability of the server or data that is managed by the server.

-OUTfile

Specifies that output from a server query is displayed in one row. If the output in a row exceeds the column width that is defined by the server, the output is displayed on multiple lines in that row. This option is available in batch mode only.

-OUTfile=filename

Specifies that output from a server query is redirected to a specified file. In batch mode, output is redirected to a file you specify and the format of the output matches the format of the output on your screen.

In interactive, console, or mount mode sessions, output displays on your screen.

-PAssword=password

Specifies the administrator's password.

-Quiet

Specifies that IBM Spectrum Protect does not display standard output messages to your screen. However, when you use this option, certain error messages still appear.

AIX Linux -SErveraddress

AIX Linux Specifies the server stanza in the dsm.sys file. The client uses the server stanza to determine the server it connects to. The SERVERADDRESS option is supported by administrative clients that are running on UNIX, Linux, and Macintosh operating systems only.

-TABdelimited

Specifies that any tabular output from a server query is to be formatted as tab-separated strings rather than in readable format. This option is intended to be used primarily when you redirect the output of an SQL query (SELECT command). The tab-separated value format is a standard data format, which can be processed by many common programs, including spreadsheets, databases, and report generators.

-TCPPort

Specifies a TCP/IP port address for an IBM Spectrum Protect server. The TCPPORT option is only supported by administrative clients that are running on Windows operating systems and is valid on the Windows administrative client command line.

-TCPServeraddress
: Specifies a TCP/IP server address for an IBM Spectrum Protect server. The TCPSERVERADDRESS option is only supported by administrative clients that are running on Windows operating systems and is valid on the Windows administrative client command line.

In addition to the options that are listed here, you can also specify any option that is in the client options file. Each option must be preceded with a hyphen and delimited with a space.

Issuing commands from the Operations Center

From the Operations Center command-line interface, you can issue commands to manage IBM Spectrum Protect™ servers that are configured as hub or spoke servers.

Procedure

To open the command-line interface, hover over the globe icon  in the Operations Center menu bar, and click Command Builder.

Issuing commands from the server console

IBM Spectrum Protect™ provides a user ID named SERVER_CONSOLE that allows you to issue commands and administer the server from the server console after IBM Spectrum Protect is installed. At installation, SERVER_CONSOLE is automatically registered as an administrator and is given system authority.

About this task

If you have system privilege, you can revoke or grant new privileges to the SERVER_CONSOLE user ID. You cannot take any of the following actions:

- Register or update the SERVER_CONSOLE user ID
- Lock or unlock the SERVER_CONSOLE user ID
- Rename the SERVER_CONSOLE user ID
- Remove SERVER_CONSOLE user ID
- Route commands from the SERVER_CONSOLE user ID

Not all IBM Spectrum Protect commands are supported by the server console. You cannot specify the WAIT parameter from the server console.

Entering administrative commands

Commands consist of command names and usually parameters and variables. Syntax diagrams depict the rules to follow when entering commands.

About this task

To display command-line help for server commands that have unique names, you can type `help` *`commandName`*, where *commandName* is the name of the server command for which you want information. For example, to display help for the REGISTER NODE command, type `help` *`register node`*. Command syntax and parameter descriptions are displayed in the output.

You can also type `help` followed by the topic number for the command. Topic numbers are listed in the table of contents for command-line help, for example:

```
3.0 Administrative commands
  3.46 REGISTER
     3.46.1 REGISTER ADMIN (Register an administrator)
     3.46.2 REGISTER LICENSE (Register a new license)
     3.46.3 REGISTER NODE (Register a node)
```

To display help about the REGISTER NODE command, type:

```
help 3.46.3
```

Use topic numbers to display command-line help for subcommands. DEFINE DEVCLASS is an example of a command that has subcommands. For example, you can specify the DEFINE DEVCLASS command for 3590 device classes and for 3592 device classes:

```
3.0 Administrative commands
  ...
  3.13.10 DEFINE DEVCLASS (Define a device class)
      3.13.10.1 DEFINE DEVCLASS (Define a 3590 device class)
      3.13.10.2 DEFINE DEVCLASS (Define a 3592 device class)
      ...
```

To display help for the DEFINE DEVCLASS command for 3590 device classes, type:

```
help 3.13.10.1
```

- Reading syntax diagrams
  To read a syntax diagram for entering a command, follow the path of the line. Read from left to right and from top to bottom.
- Using continuation characters to enter long commands
  Continuation characters are useful when you want to process a command that is longer than your screen or window width. You can use continuation characters in the interactive mode of the administrative client.
- Naming IBM Spectrum Protect objects
  IBM Spectrum Protect restricts the number and type of characters that you can use to name objects.
- Using wildcard characters to specify object names
  In some commands, such as the query commands, you can use wildcard characters to create a pattern-matching expression that specifies more than one object. Using wildcard characters makes it easier to tailor a command to your needs.
- Specifying descriptions in keyword parameters
  If a description (a string of text) for a parameter begins with a single or double quotation mark, or contains any embedded blanks or equal signs, you must surround the value with either single (') or double (") quotation marks.

Reading syntax diagrams

To read a syntax diagram for entering a command, follow the path of the line. Read from left to right and from top to bottom.

- The >>--- symbol indicates the beginning of a syntax diagram.
- The ---> symbol at the end of a line indicates that the syntax diagram continues onto the next line.
- The >--- symbol at the beginning of a line indicates that a syntax diagram continues from the previous line.
- The --->< symbol indicates the end of a syntax diagram.

Command names

The command name can consist of a single action word, such as HALT, or it can consist of an action word and an object for the action, such as DEFINE DOMAIN. You can enter the command in any column of the input line.

Enter the entire command name or the abbreviation that is specified in the syntax diagram for the command. Uppercase letters denote the shortest acceptable abbreviation. If a command appears entirely in uppercase letters, you cannot abbreviate it. You can enter the command in uppercase letters, lowercase letters, or any combination. In this example, you can enter CMDNA, CMDNAM, or CMDNAME in any combination of uppercase and lowercase letters.

```
>>-CMDNAme-----------------------------------------------------><
```

Note: Command names in descriptive text are always capitalized.

Required parameters

When a parameter is on the same line as the command name, the parameter is required. When two or more parameter values are in a stack and one of them is on the line, you *must* specify one value.

In this example, you must enter PARMNAME=A, PARMNAME=B, or PARMNAME=C. Do not include any blanks immediately before or after the equal sign (=).

```
>>-PARMName--=--+-A-+-----------------------------------------><
                +-B-+
                '-C-'
```

Optional parameters

When a parameter is below the line, the parameter is optional. In this example, you can enter PARMNAME=A or nothing at all. Do not include any blanks immediately before or after the equal sign (=).

```
>>-+----------------+-----------------------------------------><
   '-PARMName--=--A-'
```

When two or more parameter values are in a stack below the line, all of them are optional. In this example, you can enter PARMNAME=A, PARMNAME=B, PARMNAME=C, or nothing at all. Do not include any blanks immediately before or after the equal sign (=).

```
>>-+--------------------+-------------------------------------><
   '-PARMNAme--=--+-A-+-'
                  +-B-+
                  '-C-'
```

Defaults

Defaults are above the line. The system uses the default unless you override it. You can override the default by entering an option from the stack below the line.

In this example, PARMNAME=A is the default. You can also enter PARMNAME=A, PARMNAME=B, or PARMNAME=C. Do not include any blanks before or after the equal sign (=).

```
   .-PARMNAme--=--A-----.
>>-+--------------------+-------------------------------------><
   '-PARMName--=--+-A-+-'
                  +-B-+
                  '-C-'
```

Variables

Highlighted lowercase items (like this) denote variables. In these examples, var_name represents variables::

```
>>-CMDNAme--var_name-----------------------------------------><
```

```
>>-+----------------------+---------------------------------><
   '-PARMname--=--var_name-'
```

Special characters

You must code these symbols exactly as they appear in the syntax diagram.

*
: Asterisk

:
: Colon

,
: Comma

=
: Equal sign

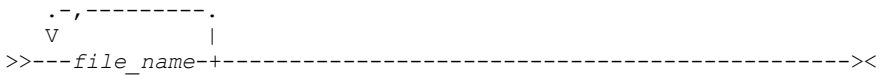
-
: Hyphen

( )
: Parentheses

.
: Period

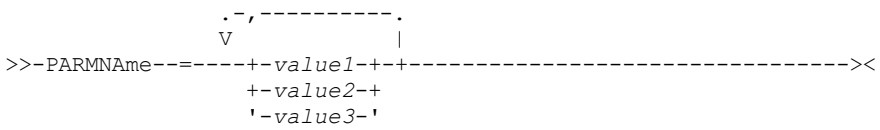
Repeating values

An arrow returning to the left means that the item can be repeated. A character within the arrow means that you must separate repeated items with that character.



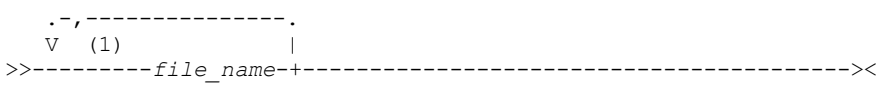
Repeatable choices

A stack of values followed by an arrow returning to the left means that you can select more than one value or, when permitted, repeat a single item. In this example, you can choose more than one value, with each name delimited with a comma. Do not include any blanks before or after the equal sign (=).



Footnotes

Footnotes are enclosed in parentheses.

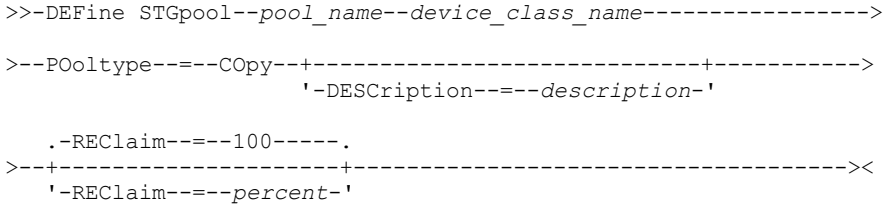


Notes:

1. You can specify up to five file names.

Entering parameters

The order in which you enter parameters can be important. The following example shows a portion of the command for defining a copy storage pool:



The first two parameters in this command (*pool_name* and *device_class_name* are required parameters. *pool_name* and *device_class_name* are also positional. That is, they must be entered in the order shown, immediately after the command name. The POOLTYPE parameter is a required keyword parameter. DESCRIPTION and RECLAIM, are optional keyword parameters. Keyword parameters are identified by an equal sign that specifies a specific value or a variable. Keyword parameters must follow any positional parameters in a command.

The following command entries, in which the keyword parameters are ordered differently, are both acceptable:

```
define stgpool mycopypool mydeviceclass pooltype=copy description=engineering
   reclaim=50
define stgpool mycopypool mydeviceclass description=engineering pooltype=copy
   reclaim=50
```

The following example, in which one of the positional parameters follows a keyword parameter, is not acceptable:

```
define stgpool mycopypool pooltype=copy mydeviceclass description=engineering
   reclaim=50
```

Syntax fragments

Some diagrams, because of their length, must display parts of the syntax with fragments. The fragment name appears between vertical bars in the diagram.

The expanded fragment appears in the diagram after all other parameters or at the bottom of the diagram. A heading with the fragment name identifies the expanded fragment. Commands appearing directly on the line are required.

In this example, the fragment is named "Fragment".

```
>>-| Fragment |-------------------------------------------------><

Fragment

   .-A-.
|--+---+-------------------------------------------------------|
   +-B-+
   '-C-'
```

Using continuation characters to enter long commands

Continuation characters are useful when you want to process a command that is longer than your screen or window width. You can use continuation characters in the interactive mode of the administrative client.

About this task

Without continuation characters, you can enter up to 256 characters. With continuation characters, you can enter up to 1500 characters.

Note: In the MACRO command, the maximums apply after any substitution variables have been applied.
With continuation characters, you can do the following:

- Enter a dash at the end of the line you want to continue.
  For example:

  ```
  register admin pease mypasswd -
  contact="david, ext1234"
  ```

- Continue a list of values by entering a dash or a back slash, with no preceding blank spaces, after the last comma of the list that you enter on the first line. Then, enter the remaining items in the list on the next line with no preceding blank spaces.
  For example:

  ```
  stgpools=stg1,stg2,stg3,-
  stg4,stg5,stg6
  ```

- Continue a string of values that are enclosed in quotation marks by entering the first part of the string that is enclosed in quotation marks, followed by a dash or a back slash at the end of the line. Then, enter the remainder of the string on the next line, enclosed in the same type of quotation marks.
  For example:

  ```
  contact="david pease, bldg. 100, room 2b, san jose,"-
  "ext. 1234, alternate contact-norm pass,ext 2345"
  ```

IBM Spectrum Protect™ concatenates the two strings with no intervening blanks. You must use only this method to continue a quoted string of values across more than one line.

Naming IBM Spectrum Protect objects

IBM Spectrum Protect™ restricts the number and type of characters that you can use to name objects.

About this task

The following characters are available for defining object names.

Character	Description
A–Z	Any letter, A through Z
0–9	Any number, 0 through 9
_	Underscore
.	Period
-	Hyphen
+	Plus
&	Ampersand

The following table shows the maximum length of characters permitted for naming objects.

Type of Name	Maximum Length
Administrators, client option sets, client nodes, passwords, server groups, server, names, virtual file space names	64
Restartable export identifiers	64
High-level and low-level TCP/IP (IPv4 or IPv6) addresses	64
Device classes, drives, libraries, management classes, policy domains, profiles, schedules scripts, backup sets, storage pools	30

The following characters are available for defining password names:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Passwords considered "LOCAL" are those passwords that authenticate with the IBM Spectrum Protect server and are not case-sensitive. Once a node or administrator is updated to use the SESSIONSECURITY=STRICT parameter, the password becomes case-sensitive the next time you change the it. Passwords considered "LDAP" are those passwords that authenticate with an LDAP directory server and are case-sensitive.

When you use DEFINE commands to define database, recovery log, and storage pool volumes, the naming convention for the volume name is dependent on the type of sequential access media or random access media that you are using. Refer to the specific VOLUME command for details.

Using wildcard characters to specify object names

In some commands, such as the query commands, you can use wildcard characters to create a pattern-matching expression that specifies more than one object. Using wildcard characters makes it easier to tailor a command to your needs.

About this task

The wildcard characters you use depend on the operating system from which you issue commands. For example, you can use wildcard characters such as an asterisk (*) to match any (0 or more) characters, or you can use a question mark (?) or a percent sign (%) to match exactly one character.

Table 1 provides references to wildcard characters for some operating systems. Use wildcard characters appropriate for your system.

Table 1. Wildcard characters by operating system

Operating system	Match any	Match exactly one
AIX®, Linux, Windows	*	?
TSO	*	%

For example, if you want to query all the management classes whose names begin with DEV in all the policy sets in DOMAIN1, and your system uses an asterisk as the *match-any* character, you can enter:

```
query mgmtclass domain1 * dev*
```

If your system uses a question mark as the *match-exactly-one* character, and you want to query the management classes in POLICYSET1 in DOMAIN1, you can enter:

```
query mgmtclass domain1 policyset1 mc?
```

IBM Spectrum Protect™ displays information about management classes with names MC.

Table 2 shows additional examples of using wildcard characters to match any characters.

Table 2. Match-any character

Pattern	Matches	Does not match
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers

Table 3 shows additional examples of using wildcard characters to match exactly one character. The question mark (?) can be replaced by a percent sign (%) if your platform uses that character instead of (?).

Table 3. Match-exactly-one character

Pattern	Matches	Does not match
ab?	abc	ab, abab, abzzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkkrs

Specifying descriptions in keyword parameters

If a description (a string of text) for a parameter begins with a single or double quotation mark, or contains any embedded blanks or equal signs, you must surround the value with either single (') or double (") quotation marks.

About this task

The opening and closing quotation marks must be the same type of quotation marks. For example, if the opening quotation is a single quotation mark, the closing quotation mark must also be a single quotation mark.

For example, to register a new client node named Louie, with a password of secret, and with his title included as contact information, enter:

```
register node louie secret contact="manager of dept. 61f"
```

The following table presents ways of entering a description for the CONTACT parameter. The value can contain quotation marks, embedded blanks, or equal signs.

For this description	Enter this
manager	contact=manager
manager's	contact="manager's" *or* contact='manager"s'

For this description	Enter this
"manager"	contact='"manager"' *or* contact="""manager"""
manager's report	contact="manager's report" *or* contact='manager''s report'
manager's "report"	contact='manager''s "report"'
manager=dept. 61f	contact='manager=dept. 61f'
manager reports to dept. 61f	contact='manager reports to dept. 61f' *or* contact="manager reports to dept. 61f"

Controlling command processing

You can run some IBM Spectrum Protect™ commands sequentially or concurrently with other commands. You can also route commands from one server to other servers for processing.

About this task

- Server command processing
  IBM Spectrum Protect processes administrator commands either in the foreground or in the background. Commands that process in the foreground must complete before you can issue another command. When commands are processing in the background, you can issue additional commands at any time.
- Stopping background processes
  Use the CANCEL PROCESS command to cancel commands that generate background processes.

Server command processing

IBM Spectrum Protect™ processes administrator commands either in the foreground or in the background. Commands that process in the foreground must complete before you can issue another command. When commands are processing in the background, you can issue additional commands at any time.

Most IBM Spectrum Protect commands process in the foreground. For some commands that normally process in the background (for example, BACKUP DB), you can specify the WAIT parameter (WAIT=YES) with the command so that the command processes in the foreground. You might want to process a command in the foreground rather than in the background for any of the following reasons:

- To quickly determine whether a command completed successfully. When you issue a command that processes in the foreground, IBM Spectrum Protect sends a confirmation message that indicates that the command completed successfully. If you process the command in the background, you need to open operational reporting or query the activity log to determine whether the command completed successfully.
- To monitor server activities (for example, messages) on the administrative client as a command is being processed. This might be preferable to searching a long activity log after the command has completed.
- To be able to start another process immediately after a command completed. For example, you might specify WAIT=YES for a command that takes a short time to process so that, when the processing completes, you can immediately start processing another command.
- To serialize commands in an administrative script when it is important that one command completes before another begins.

Check the individual command description to determine whether a command has a WAIT parameter.

You can cancel commands that are processed in the foreground from the server console or from another administrative client session.

Each background process is assigned a process number. Use the QUERY PROCESS command to obtain the status and process number of a background process.

Note:

- If you are defining a schedule with a command that specifies WAIT=NO (the default), and you issue QUERY EVENT to determine the status of your scheduled operation, failed operations report an event status of COMPLETED with a return of OK. In order for the QUERY EVENT output to reflect the failed status, the WAIT parameter must be set to YES. This runs the scheduled operation in the foreground and informs you of the status when it completes.
- You cannot process commands in the foreground from the server console.

Stopping background processes

Use the CANCEL PROCESS command to cancel commands that generate background processes.

About this task

Use the QUERY PROCESS command to obtain the status and process number of a background process. If a background process is active when you cancel it, the server stops the process. Any changes that are uncommitted are rolled back. However, changes that are committed are not rolled back.

When you issue a QUERY command from the administrative client, multiple screens of output might be generated. If this occurs and additional output is not needed, you can cancel the display of output to the client workstation. Doing so does not end the processing of the command.

Performing tasks concurrently on multiple servers

Command routing allows you to route commands to one or more servers for processing and then collect the output from these servers.

About this task

To route commands to other servers, you must have the same administrator ID and password as well as the required administrative authority on each server to which the command is being routed. You cannot route commands to other servers from the server console.

After the command has completed processing on all servers, the output displays, in its entirety, for each server. For example, the output from SERVER_A displays in its entirety, followed by the output from SERVER_B. The output includes summary messages for each individual server and identifies which server processed the output. Return codes indicate whether commands processed on the servers successfully. These return codes include one of three severities: 0, ERROR, or WARNING.

Each server that is identified as the target of a routed command must first be defined using the DEFINE SERVER command. The command is automatically routed to all servers specified as members of a server group or to individual servers specified with the command.

The following examples describe how to route the QUERY STGPOOL command to one server, multiple servers, a server group, multiple server groups, or a combination of servers and server groups. Each server or server group in a list must be separated with a comma, without spaces.

Routing commands to a single server

Procedure

To route the QUERY STGPOOL command to a server named ASTRO, enter:

```
astro: query stgpool
```

The colon after the server name indicates the end of the routing information. This is also called the *server prefix*. Another way to indicate the end of routing information is to use parentheses around the server name, for example:

```
(astro) query stgpool
```

Routing commands to multiple servers

About this task

Procedure

To route the QUERY STGPOOL command to multiple servers named HD_QTR, MIDAS, SATURN, enter:

```
hd_qtr,midas,saturn: query stgpool
```

If the first server has not been defined to IBM Spectrum Protect, the command is routed to the next defined server in the list of servers.

You can also enter the command this way:

```
(hd_qtr,midas,saturn) query stgpool
```

Routing commands to a server group

About this task

In this example, the server group ADMIN has servers named SECURITY, PAYROLL, PERSONNEL defined as group members. The command is routed to each of these servers.

Procedure

To route the QUERY STGPOOL command to the server group named ADMIN, enter:

```
admin: query stgpool
```

You can also enter the command this way:

```
(admin) query stgpool
```

Routing commands to server groups

About this task

In this example, the server group ADMIN2 has servers SERVER_A, SERVER_B, and SERVER_C defined as group members, and server group ADMIN3 has servers ASTRO, GUMBY, and CRUSTY defined as group members. The command is routed to servers SERVER_A, SERVER_B, SERVER_C, ASTRO, GUMBY, and CRUSTY.

Procedure

To route the QUERY STGPOOL command to two server groups that are named ADMIN2 and ADMIN3, enter:

```
admin2,admin3: query stgpool
```

You can also enter the command this way:

```
(admin2,admin3) query stgpool
```

Routing commands to two servers and a server group

About this task

In this example, the server group DEV_GROUP has servers SALES, MARKETING, and STAFF defined as group members. The command is routed to servers SALES, MARKETING, STAFF, MERCURY, and JUPITER.

Procedure

To route the QUERY STGPOOL command to a server group named DEV_GROUP and to the servers named MERCURY and JUPITER, enter:

```
dev_group,mercury,jupiter: query stgpool
```

You can also enter the command this way:

```
(dev_group,mercury,jupiter) query stgpool
```

Routing commands inside scripts

About this task

When routing commands inside scripts, you must enclose the server or server group in parentheses and omit the colon. Otherwise, the command will not be routed when the RUN command is issued, and will only be run on the server where the RUN

command is issued.

For example, to route the QUERY STGPOOL command inside a script:

Procedure

1. Define a script called QU_STG to route it to the DEV_GROUP server group.

   ```
   define script qu_stg "(dev_group) query stgpool"
   ```

2. Run the QU_STG script:

   ```
   run qu_stg
   ```

Results

In this example, the server group DEV_GROUP has servers SALES, MARKETING, and STAFF defined as group members. The QUERY STGPOOL command is routed to these servers.

Privilege classes for commands

The authority granted to an administrator through the privilege class determines which administrative commands that the administrator can issue.

There are four administrator privilege classes in IBM Spectrum Protect™:

- System
- Policy
- Storage
- Operator

After an administrator has been registered using the REGISTER ADMIN command, the administrator can issue a limited set of commands, including all query commands. When you install IBM Spectrum Protect, the server console is defined as a system administrator named SERVER_CONSOLE and is granted system privilege.

- Commands requiring system privilege
  An administrator with system privilege has the highest level of authority for the server. With system privilege, an administrator can issue any administrative command and has authority to manage all policy domains and all storage pools.
- Commands requiring policy privilege
  An administrator with policy privilege can issue commands that relate to policy management objects such as policy domains, policy sets, management classes, copy groups, and schedules. The policy privilege can be unrestricted, or can be restricted to specific policy domains.
- Commands requiring storage privilege
  An administrator with storage privilege can issue commands that allocate and control storage resources for the server. The storage privilege can be unrestricted, or can be restricted to specific storage pools.
- Commands requiring operator privilege
  An administrator with operator privilege can issue commands that control the immediate operation of the server and the availability of storage media.
- Commands any administrator can issue
  A limited number of commands can be used by any administrator, even if that administrator has not been granted any specific administrator privileges.

Commands requiring system privilege

An administrator with system privilege has the highest level of authority for the server. With system privilege, an administrator can issue any administrative command and has authority to manage all policy domains and all storage pools.

Table 1 lists the commands that administrators with system privilege can issue. In some cases administrators with lower levels of authority, for example, unrestricted storage privilege, can also issue these commands. In addition, the REQSYSAUTHOUTFILE server option can be used to specify that certain commands require system privilege if they cause the server to write to an external file. For more information about this server option, review REQSYSAUTHOUTFILE.

Table 1. System privilege commands

Command name	Command name
• AUDIT LDAPDIRECTORY • AUDIT LICENSES • ACCEPT DATE • BEGIN EVENTLOGGING • CANCEL EXPIRATION • CANCEL PROCESS • CANCEL REPLICATION • CANCEL REQUEST • CANCEL RESTORE • CLEAN DRIVE • COPY ACTIVEDATA • COPY DOMAIN • COPY POLICYSET • COPY PROFILE • COPY SCHEDULE (Review note.) • COPY SCRIPT • COPY SERVERGROUP • DEFINE BACKUPSET • DEFINE CLIENTACTION • DEFINE CLIENTOPT • DEFINE CLOPTSET • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DEFINE DEVCLASS • DEFINE DOMAIN • DEFINE DRIVE • DEFINE EVENTSERVER • DEFINE GRPMEMBER • DEFINE LIBRARY • DEFINE MACHINE • DEFINE MACHNODEASSOCIATION • DEFINE NODEGROUP • DEFINE NODEGROUPMEMBER • DEFINE PATH • DEFINE PROFASSOCIATION • DEFINE PROFILE • DEFINE RECMEDMACHASSOCIATION • DEFINE RECOVERYMEDIA • DEFINE SCHEDULE (Review note.) • DEFINE SCRIPT • DEFINE SERVER • DEFINE SERVERGROUP	• DEFINE SPACETRIGGER • DEFINE STGPOOL • DEFINE SUBSCRIPTION • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME • DELETE BACKUPSET • DELETE CLIENTOPT • DELETE CLOPTSET • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DELETE DOMAIN • DELETE DRIVE • DELETE EVENTSERVER • DELETE GRPMEMBER • DELETE LIBRARY • DELETE MACHINE • DELETE MACHNODEASSOCIATION • DELETE NODEGROUP • DELETE NODEGROUPMEMBER • DELETE PROFASSOCIATION • DELETE PROFILE • DELETE RECMEDMACHASSOCIATION • DELETE RECOVERYMEDIA • DELETE SCHEDULE (Review note.) • DELETE SCRIPT • DELETE SERVER • DELETE SERVERGROUP • DELETE SPACETRIGGER • DELETE STGPOOL • DELETE SUBSCRIBER • DELETE SUBSCRIPTION • DELETE VIRTUALFSMAPPING • DISABLE EVENTS • ENABLE EVENTS • END EVENTLOGGING • EXPIRE INVENTORY • EXPORT ADMIN • EXPORT NODE • EXPORT POLICY • EXPORT SERVER • GENERATE BACKUPSET • GRANT AUTHORITY

Command name	Command name
• GRANT PROXYNODE • IDENTIFY DUPLICATES • IMPORT NODE • IMPORT POLICY • IMPORT SERVER • INSERT MACHINE • LABEL LIBVOLUME • LOCK ADMIN • LOCK PROFILE • MIGRATE STGPOOL • MOVE DRMEDIA • MOVE MEDIA • MOVE GRPMEMBER • NOTIFY SUBSCRIBERS • PERFORM LIBACTION • PING SERVER • PREPARE • QUERY BACKUPSETCONTENTS • QUERY MEDIA • QUERY RPFCONTENT • QUERY TOC • RECLAIM STGPOOL • RECONCILE VOLUMES • REGISTER ADMIN • REGISTER LICENSE • REMOVE ADMIN • REMOVE REPLNODE • RENAME ADMIN • RENAME SCRIPT • RENAME SERVERGROUP • RENAME STGPOOL • REPLICATE NODE • RESET PASSEXP • RESTORE NODE • REVOKE AUTHORITY • REVOKE PROXYNODE • RUN • SET ACCOUNTING • SET ACTLOGRETENTION • SET ARCHIVERETENTIONPROTECTION • SET ARREPLRULEDEFAULT • SET BKREPLRULEDEFAULT • SET CLIENTACTDURATION	• SET CONFIGMANAGER • SET CONFIGREFRESH • SET CONTEXTMESSAGING • SET CROSSDEFINE • SET DBRECOVERY • SET DEFAULTAUTHENTICATION • SET DRMACTIVEDATASTGPOOL • SET DRMCHECKLABEL • SET DRMCMDFILENAME • SET DRMCOPYCONTAINERSTGPOOL • SET DRMCOPYSTGPOOL • SET DRMCOURIERNAME • SET DRMDBBACKUPEXPIREDAYS • SET DRMFILEPROCESS • SET DRMINSTRPREFIX • SET DRMNOTMOUNTABLENAME • SET DRMPLANPREFIX • SET DRMPLANVPOSTFIX • SET DRMPRIMSTGPOOL • SET DRMRPFEXPIREDAYS • SET DRMVAULTNAME • SET EVENTRETENTION • SET INVALIDPWLIMIT • SET LDAPPASSWORD • SET LDAPUSER • SET LICENSEAUDITPERIOD • SET MAXCMDRETRIES • SET MAXSCHEDSESSIONS • SET MINPWLENGTH • SET PASSEXP • SET QUERYSCHEDPERIOD • SET RANDOMIZE • SET REPLRETENTION • SET REPLSERVER • SET RETRYPERIOD • SET SCHEDMODES • SET SERVERHLADDRESS • SET SERVERLLADDRESS • SET SERVERNAME • SET SERVERPASSWORD • SET SPREPLRULEDEFAULT • SET SUBFILE • SET TOCLOADRETENTION
• SETOPT • UNLOCK ADMIN • UNLOCK PROFILE • UPDATE ADMIN • UPDATE BACKUPSET • UPDATE CLIENTOPT • UPDATE CLOPTSET • UPDATE COLLOCGROUP • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE LIBVOLUME • UPDATE MACHINE	• UPDATE NODEGROUP • UPDATE PATH • UPDATE PROFILE • UPDATE RECOVERYMEDIA • UPDATE REPLRULE • UPDATE SCHEDULE (Review note.) • UPDATE SCRIPT • UPDATE SERVER • UPDATE SERVERGROUP • UPDATE SPACETRIGGER • UPDATE VIRTUALFSMAPPING • UPDATE VOLHISTORY • VALIDATE LANFREE • VALIDATE REPLICATION

Command name	Command name
Note: This command is restricted by the authority that is granted to an administrator. System privilege is required only for administrative command schedules. System or policy privilege is required for client operation schedules.	

Commands requiring policy privilege

An administrator with policy privilege can issue commands that relate to policy management objects such as policy domains, policy sets, management classes, copy groups, and schedules. The policy privilege can be unrestricted, or can be restricted to specific policy domains.

With unrestricted policy privilege, you can issue all of the administrator commands that require policy privilege. You can issue commands that affect all existing policy domains as well as any policy domains that are defined in the future. An unrestricted policy administrator cannot define, delete, or copy policy domains.

With restricted policy privilege, you can issue administrator commands that affect one or more policy domains for which authority is granted. For example, the DELETE MGMTCLASS command requires you to have policy privilege for the policy domain to which the management class belongs.

Table 1 lists the commands that an administrator with policy privilege can issue.

Table 1. Policy privilege commands

Command name	Command name
• ACTIVATE POLICYSET • ASSIGN DEFMGMTCLASS • CLEAN DRIVE • BACKUP NODE • COPY MGMTCLASS • COPY POLICYSET • COPY SCHEDULE (Review note 2.) • DEFINE ASSOCIATION • DEFINE BACKUPSET • DEFINE COPYGROUP • DEFINE CLIENTACTION • DEFINE CLIENTOPT • DEFINE MGMTCLASS • DEFINE NODEGROUP • DEFINE NODEGROUPMEMBER • DEFINE POLICYSET • DEFINE SCHEDULE • DELETE ASSOCIATION • DELETE BACKUPSET • DELETE COPYGROUP • DELETE EVENT (Review note 1.) • DELETE FILESPACE • DELETE MGMTCLASS • DELETE NODEGROUP • DELETE NODEGROUPMEMBER	• DELETE POLICYSET • DELETE PATH • DELETE SCHEDULE (Review note 2.) • GENERATE BACKUPSET • LOCK NODE • QUERY BACKUPSETCONTENTS • REGISTER NODE • REMOVE NODE • RENAME FILESPACE • RENAME NODE • SET SUMMARYRETENTION • RESTORE NODE • QUERY TOC • UNLOCK NODE • UPDATE BACKUPSET • UPDATE COPYGROUP • UPDATE DOMAIN • UPDATE MGMTCLASS • UPDATE NODE • UPDATE NODEGROUP • UPDATE POLICYSET • UPDATE SCHEDULE (Review note 2.) • VALIDATE POLICYSET
Notes: 1. This command can be restricted by policy domain. An administrator with unrestricted policy privilege or restricted policy privilege for a specified policy domain can issue this command. 2. This command is restricted by the authority that is granted to an administrator. System privilege is required only for administrative command schedules. System or policy privilege is required for client operation schedules.	

Commands requiring storage privilege

An administrator with storage privilege can issue commands that allocate and control storage resources for the server. The storage privilege can be unrestricted, or can be restricted to specific storage pools.

Unrestricted storage privilege permits you to issue all of the administrator commands that require storage privilege. You can issue commands that affect all existing storage pools as well as any storage pools that are defined in the future. You can also issue commands that affect the database and the recovery log. An unrestricted storage administrator cannot define or delete storage pools.

Restricted storage privilege permits you to issue administrator commands that only affect a storage pool for which you have been granted authority. For example, the DELETE VOLUME command only affects a storage pool volume that is defined to a specific storage pool.

Table 1 lists the commands an administrator with storage privilege can issue.

Table 1. Storage privilege commands

Command name	Command name
• AUDIT LIBRARY • AUDIT VOLUME (Review note.) • BACKUP DB • BACKUP DEVCONFIG • BACKUP STGPOOL • BACKUP VOLHISTORY • CHECKIN LIBVOLUME • CHECKOUT LIBVOLUME • COPY ACTIVEDATA (Review note.) • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DEFINE DATAMOVER • DEFINE DEVCLASS • DEFINE DRIVE • DEFINE LIBRARY • DEFINE PATH • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME (Review note.) • DEFINE SPACETRIGGER • DELETE COLLOCGROUP • DELETE COLLOCMEMBER • DELETE DATAMOVER • DELETE DEVCLASS • DELETE DRIVE • DELETE LIBRARY • DELETE PATH	• DELETE SPACETRIGGER • DELETE VIRTUALFSMAPPING • DELETE VOLHISTORY • DELETE VOLUME (Review note.) • GRANT PROXYNODE • LABEL LIBVOLUME • MIGRATE STGPOOL • MOVE DATA (Review note.) • MOVE MEDIA • QUERY TAPEALERTMSG • RECLAIM STGPOOL • RESTORE STGPOOL • RESTORE VOLUME • REVOKE PROXYNODE • SET TAPEALERTMSG • UPDATE COLLOCGROUP • UPDATE DATAMOVER • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE PATH • UPDATE SPACETRIGGER • UPDATE STGPOOL (Review note.) • UPDATE VIRTUALFSMAPPING
Note: This command can be restricted by storage pool. An administrator with unrestricted storage privilege or restricted storage privilege for a specified storage pool can issue this command.	

Commands requiring operator privilege

An administrator with operator privilege can issue commands that control the immediate operation of the server and the availability of storage media.

Table 1 lists the commands an administrator with operator privilege can issue.

Table 1. Operator privilege commands

Command Name	Command Name

Command Name	Command Name
• CANCEL SESSION • DISABLE SESSIONS • DISMOUNT VOLUME • ENABLE SESSIONS • HALT	• MOVE DRMEDIA • MOVE MEDIA • QUERY MEDIA • REPLY • UPDATE VOLUME • VARY

Commands any administrator can issue

A limited number of commands can be used by any administrator, even if that administrator has not been granted any specific administrator privileges.

Table 1 lists the commands any registered administrator can issue.

Table 1. Commands issued by all administrators

Command Name	Command Name
• COMMIT • HELP • ISSUE MESSAGE • MACRO • PARALLEL • QUERY ACTLOG • QUERY ADMIN • QUERY ASSOCIATION • QUERY AUDITOCCUPANCY • QUERY BACKUPSET • QUERY CLOPTSET • QUERY COLLOCGROUP • QUERY CONTENT • QUERY COPYGROUP • QUERY DATAMOVER • QUERY DB • QUERY DBSPACE • QUERY DEVCLASS • QUERY DIRSPACE • QUERY DOMAIN • QUERY DRIVE • QUERY DRMEDIA • QUERY DRMSTATUS • QUERY ENABLED • QUERY EVENT • QUERY EVENTRULES • QUERY EVENTSERVER • QUERY FILESPACE • QUERY LIBRARY • QUERY LIBVOLUME • QUERY LICENSE • QUERY LOG • QUERY MACHINE • QUERY MGMTCLASS • QUERY MOUNT • QUERY NASBACKUP	• QUERY NODE • QUERY NODEDATA • QUERY NODEGROUP • QUERY OCCUPANCY • QUERY OPTION • QUERY PATH • QUERY POLICYSET • QUERY PROCESS • QUERY PROFILE • QUERY PROXYNODE • QUERY RECOVERYMEDIA • QUERY REPLICATION • QUERY REPLNODE • QUERY REPLRULE • QUERY REQUEST • QUERY RESTORE • QUERY RPFILE • QUERY SCHEDULE • QUERY SCRIPT • QUERY SERVER • QUERY SERVERGROUP • QUERY SESSION • QUERY SPACETRIGGER • QUERY STATUS • QUERY STGPOOL • QUERY SUBSCRIBER • QUERY SUBSCRIPTION • QUERY SYSTEM • QUERY VIRTUALFSMAPPING • QUERY VOLHISTORY • QUERY VOLUME • QUIT • ROLLBACK • SELECT • SERIAL

Administrative commands

Administrative commands are available to manage and configure the server.

Information for each command includes:

- A description of the tasks a command performs
- The administrator privilege class required to use the command
- A syntax diagram that identifies the required and optional parameters for the command
- Descriptions of each parameter of the command
- Examples of using the command
- A list of related commands

- ACCEPT DATE (Accepts the current system date)
  Use this command to allow the server to begin normal processing, when the server does not start normal processing because of a discrepancy between the server date and the current date on the system.
- ACTIVATE POLICYSET (Activate a new policy set)
  Use this command to copy the contents of a policy set to the ACTIVE policy set for the domain. The server uses the rules in the ACTIVE policy set to manage client operations in the domain. You can define multiple policy sets for a policy domain, but only one policy set can be active. The current ACTIVE policy set is replaced by the one you specify when you issue this command. You can modify the ACTIVE policy set only by activating another policy set.
- ASSIGN DEFMGMTCLASS (Assign a default management class)
  Use this command to specify a management class as the default management class for a policy set. You must assign a default management class for a policy set before you can activate that policy set.
- AUDIT commands
  Use the AUDIT commands to review or examine the adequacy of the database information and the storage pool volume. The AUDIT LDAPDIRECTORY command deletes nodes or administrator IDs from an LDAP directory server, that do not authenticate their passwords with the LDAP directory server.
- BACKUP commands
  Use the BACKUP commands to create backup copies of IBM Spectrum Protect™ information or objects.
- BEGIN EVENTLOGGING (Begin logging events)
  Use this command to begin logging events to one or more receivers. A receiver for which event logging has begun is an *active receiver*.
- CANCEL commands
  Use the CANCEL commands to end a task or process before it is completed.
- CHECKIN LIBVOLUME (Check a storage volume into a library)
  Use this command to add a sequential access storage volume or a cleaning tape to the server inventory for an automated library. The server cannot use a volume that physically resides in an automated library until that volume is checked in.
- CHECKOUT LIBVOLUME (Check a storage volume out of a library)
  Use this command to remove a sequential access storage volume from the server inventory for an automated library. This command creates a background process that can be canceled with the CANCEL PROCESS command. To display information on background processes, use the QUERY PROCESS command.
- CLEAN DRIVE (Clean a drive)
  Use this command when you want IBM Spectrum Protect to immediately load a cleaner cartridge into a drive regardless of the cleaning frequency.
- COMMIT (Control committing of commands in a macro)
  Use this command to control when a command is committed in a macro and to update the database when commands complete processing. When issued from the console mode of the administrative client, this command does not generate a message.
- CONVERT STGPOOL (Convert a storage pool to a container storage pool)
  Use this command to convert a primary storage pool that uses a FILE device class, a tape device class, or a virtual tape library (VTL) to a directory-container or a cloud-container storage pool. You can use container storage pools for both inline and client-side data deduplication.
- COPY commands
  Use the COPY commands to create a copy of IBM Spectrum Protect objects or data.
- DEACTIVATE DATA (Deactivate data for a client node)
  Use this command to specify that active data that was backed up for an application client node before a specified date is no longer needed. The command marks the data as inactive so it can be deleted according to your data retention policies.
- DECOMMISSION commands
  Use the DECOMMISSION commands to remove client nodes from the production environment. Client nodes include applications, systems, and virtual machines.
- DEFINE commands
  Use the DEFINE commands to create IBM Spectrum Protect objects.
- DELETE commands
  Use the DELETE commands to delete or remove an IBM Spectrum Protect object.

- DISABLE commands
  Use DISABLE commands to prevent some types of operations by the server.
- DISMOUNT command
  Use the DISMOUNT command to dismount a volume by the real device address or by volume name.
- DISPLAY OBJNAME (Display a full object name)
  Use this command when you want IBM Spectrum Protect to display a full object name if the name displayed in a message or query output has been abbreviated due to length. Object names that are very long can be difficult to display and use through normal operating system facilities. The IBM Spectrum Protect server will abbreviate long names and assign them a token ID which might be used if the object path name exceeds 1024 bytes. The token ID is displayed in a string that includes identifiers for the node, filespace, and object name. The format is: [TSMOBJ:*nID.fsID.objID*]. When specified with the DISPLAY OBJNAME command, the token ID can be used to show the full object name.
- ENABLE commands
  Use ENABLE commands to allow some types of operations by the server.
- ENCRYPT STGPOOL (Encrypt data in a storage pool)
  Use this command to encrypt data in a directory-container or cloud-container storage pool.
- END EVENTLOGGING (Stop logging events)
  Use this command to stop logging events to an active receiver.
- EXPIRE INVENTORY (Manually start inventory expiration processing)
  Use this command to manually start inventory expiration processing. The inventory expiration process removes client backup and archive file copies from server storage. Removal is based on policy specifications in the backup and archive copy groups of the management classes to which the files are bound.
- EXPORT commands
  Use the EXPORT commands to copy information from an IBM Spectrum Protect server to sequential removable media.
- EXTEND DBSPACE (Increase space for the database)
  Use this command to increase space for the database by adding directories for the database to use.
- GENERATE commands
  Use the GENERATE commands for backup sets for a selected filespace or client node.
- GRANT commands
  Use the GRANT command to grant appropriate privileges or access.
- HALT (Shut down the server)
  Use this command to shut down the server. The HALT command forces an abrupt shutdown, which cancels all the administrative and client node sessions even if they are not completed.
- HELP (Get help on commands and error messages)
  Use this command to display administrative commands and error messages. You can issue the command from an administrative command line client.
- IDENTIFY DUPLICATES (Identify duplicate data in a storage pool)
  Use this command to start or stop processes that identify duplicate data in a storage pool. You can specify the number of duplicate-identification processes and their duration.
- IMPORT commands
  Use the IMPORT commands to import information from export media to an IBM Spectrum Protect server.
- INSERT MACHINE (Insert machine characteristics information or recovery instructions)
  Use this command to add client machine characteristics or recovery instructions to existing machine information in the database.
- ISSUE MESSAGE (Issue a message from a server script)
  Use this command with return code processing in a script to issue a message from a server script to determine where the problem is with a command in the script.
- LABEL LIBVOLUME (Label a library volume)
  Use this command to label tape volumes or, in an automated library, to label the volumes automatically as they are checked in. With this command, the server uses the full-length label with which the volumes are often prelabeled.
- LOAD DEFALERTTRIGGERS (Load the default set of alert triggers)
  Use this command to load the default set of alert triggers to the IBM Spectrum Protect server.
- LOCK commands
  Use the LOCK command to prevent users from accessing the server.
- MACRO (Invoke a macro)
  Use this command to invoke a file from the administrative command line that contains one or more IBM Spectrum Protect administrative commands to be performed.
- MIGRATE STGPOOL (Migrate storage pool to next storage pool)
  Use this command to migrate files from one storage pool to the next storage pool in the storage hierarchy.
- MOVE commands
  Use the MOVE commands to either transfer backup or archive data between storage pools, or to move disaster recovery media on and off site.

- NOTIFY SUBSCRIBERS (Notify managed servers to update profiles)
  Use this command on a configuration manager to notify one or more managed servers to request that their configuration information be immediately refreshed.
- PERFORM LIBACTION (Define or delete all drives and paths for a library)
  Use this command to define or delete all drives and their paths for a single library in one step.
- PING SERVER (Test the connection between servers)
  Use this command to test the connection between the local server and a remote server.
- PREPARE (Create a recovery plan file)
  Use this command to create a recovery plan file, which contains the information that is needed to recover an IBM Spectrum Protect server. You can store a recovery plan file on a file system that is accessible to the source server or on a target server.
- PROTECT STGPOOL (Protect data that belongs to a storage pool)
  Use this command to protect data in a directory-container storage pool by storing a copy of the data in another storage pool on a replication target server or on the same server by protecting the data to tape. When you protect the directory-container storage pool, you can later try to repair damage in the storage pool by using the REPAIR STGPOOL command.
- QUERY commands
  Use the QUERY commands to request or display information about IBM Spectrum Protect objects.
- QUIT (End the interactive mode of the administrative client)
  Use this command to end an administrative client session in interactive mode.
- RECLAIM STGPOOL (Reclaim volumes in a sequential-access storage pool)
  Use this command to reclaim volumes in a sequential-access storage pool. Reclamation does not move inactive versions of backup data from volumes in active-data pools.
- RECONCILE VOLUMES (Reconcile differences in the virtual volume definitions)
  Issue this command from the source server to reconcile differences between virtual volume definitions on the source server and archive files on the target server. IBM Spectrum Protect finds all volumes of the specified device class on the source server and all corresponding archive files on the target server. The target server inventory is also compared to the local definition for virtual volumes to see if inconsistencies exist.
- REGISTER commands
  Use the REGISTER commands to define or add objects to IBM Spectrum Protect.
- REMOVE commands
  Use the REMOVE commands to remove an object from IBM Spectrum Protect.
- RENAME commands
  Use the RENAME commands to change the name of an existing object.
- REPAIR STGPOOL (Repair a directory-container storage pool)
  Use this command to repair deduplicated extents in a directory-container storage pool. Damaged deduplicated extents are repaired with extents that are backed up to the target replication server or to container-copy storage pools on the same server.
- REPLICATE NODE (Replicate data in file spaces that belong to a client node)
  Use this command to replicate data in file spaces that belong to one or more client nodes or defined groups of client nodes.
- REPLY (Allow a request to continue processing)
  Use this command and an identification number to inform the server that you have completed a requested operation. Not all server requests require a reply. This command is required only if the request message specifically indicates that a reply is needed.
- RESET PASSEXP (Reset password expiration)
  Use the RESET PASSEXP command to reset the password expiration period to the common expiration period for administrator and client node passwords. The RESET PASSEXP command does not apply to passwords that are stored on an LDAP directory server.
- RESTART EXPORT (Restart a suspended export operation)
  Use this command to restart a suspended export operation.
- RESTORE commands
  Use the RESTORE commands to restore IBM Spectrum Protect storage pools or volumes.
- REVOKE commands
  Use the REVOKE commands to revoke privileges or access.
- ROLLBACK (Rollback uncommitted changes in a macro)
  Use this command within a macro to undo any processing changes made by commands run by the server but not yet committed to the database. A committed change is permanent and cannot be rolled back. The ROLLBACK command is useful for testing macros.
- RUN (Run an IBM Spectrum Protect script)
  Use this command to run an IBM Spectrum Protect script. To issue this command on another server, the script being run must be defined on that server.
- SELECT (Perform an SQL query of the IBM Spectrum Protect database)
  Use the SELECT command to create and format a customized query of the IBM Spectrum Protect database.

- SET commands
  Use the SET commands to specify values that affect many different IBM Spectrum Protect operations.
- SETOPT (Set a server option for dynamic update)
  You can use the SETOPT command to update most server options dynamically without stopping and restarting the server. For the DBDIAGLOGSIZE option, you must stop and start the server. A SETOPT command contained in a macro or a script cannot be rolled back.
- SHRED DATA (Shred data)
  Use this command to manually start the process of shredding deleted sensitive data. Manual shredding is possible only if automatic shredding is disabled.
- SUSPEND EXPORT (Suspend a currently running export operation)
  Use this command to suspend a currently running server-to-server export operation which has a FILEDATA value that is not NONE. The export operation that you want to suspend must be past the initialization phase to be eligible for suspension. The state of the export operation is saved. The operation can be restarted by issuing the RESTART EXPORT command.
- UNLOCK commands
  Use the UNLOCK commands to reestablish access after an object was locked.
- UPDATE commands
  Use the UPDATE command to modify one or more attributes of an existing IBM Spectrum Protect object.
- VALIDATE commands
  Use the VALIDATE command to verify that an object is complete or valid for IBM Spectrum Protect.
- VARY (Bring a random access volume online or offline)
  Use this command to make a random access storage pool volume online or offline to the server.

ACCEPT DATE (Accepts the current system date)

Use this command to allow the server to begin normal processing, when the server does not start normal processing because of a discrepancy between the server date and the current date on the system.

When the server does not start normal processing because of a discrepancy between the server date and the current date, this command forces the server to accept the current date and time as valid. If the system time is valid and the server has not been run for an extended time, this command should be run to allow the server to begin normal processing.

Attention: If the system date is invalid or the server was created or run previously with an invalid system date and this command is issued, any server processing or command that uses dates can have unexpected results. File expiration can be affected, for example. When the server is started with the correct date, files backed up with future dates will not be considered for expiration until that future date is reached. Files backed up with dates that have passed will expire faster. When the server processing encounters a future date, an error message is issued.

If the server detects an invalid date or time, server sessions become disabled (as if the DISABLE SESSIONS command had been issued). Expiration, migration, reclamation, and volume history deletion operations are not able to continue processing.

Use the ENABLE SESSIONS ALL command after you issue the ACCEPT DATE command to re-enable sessions to start.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-ACCept Date-----------------------------------------------><
```

Parameters

None.

Example: Accept the current system date

Allow the server to accept the current date as the valid date.

```
accept date
```

Related commands

Table 1. Command related to ACCEPT DATE

Command	Description
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.

ACTIVATE POLICYSET (Activate a new policy set)

Use this command to copy the contents of a policy set to the ACTIVE policy set for the domain. The server uses the rules in the ACTIVE policy set to manage client operations in the domain. You can define multiple policy sets for a policy domain, but only one policy set can be active. The current ACTIVE policy set is replaced by the one you specify when you issue this command. You can modify the ACTIVE policy set only by activating another policy set.

Before activating a policy set, check that the policy set is complete and valid by using the VALIDATE POLICYSET command.

The ACTIVATE POLICYSET command fails if any of the following conditions exist:

- A copy group specifies a copy storage pool as a destination.
- A management class specifies a copy storage pool as the destination for files that were migrated by an IBM Spectrum Protect™ for Space Management client.
- The policy set has no default management class.
- A TOCDESTINATION parameter is specified, and the storage pool is either a copy pool or has a data format other than NATIVE or NONBLOCK.

The ACTIVE policy set and the last activated policy set are not necessarily identical. You can modify the original policy set that you activated without affecting the ACTIVE policy set.

If the server has data retention protection enabled, the following conditions must exist:

- All management classes in the policy set to be activated must contain an archive copy group.
- If a management class exists in the active policy set, a management class with the same name must exist in the policy set to be activated.
- If an archive copy group exists in the active policy set, the corresponding copy group in the policy set to be activated must have a RETVER value at least as large as the corresponding values in the active copy group.

Attention: Retention protection only applies to archive objects.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-ACTivate POlicyset--domain_name--policy_set_name------------><
```

Parameters

domain_name (Required)
: Specifies the policy domain for which you want to activate a policy set.

policy_set_name (Required)
: Specifies the policy set to activate.

Example: Activate a policy set on a specific policy domain

Activate the VACATION policy set in the EMPLOYEE_RECORDS policy domain.

```
activate policyset employee_records vacation
```

Related commands

Table 1. Commands related to ACTIVATE POLICYSET

Command	Description
COPY POLICYSET	Creates a copy of a policy set.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY DOMAIN	Displays information about policy domains.
QUERY POLICYSET	Displays information about policy sets.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

ASSIGN DEFMGMTCLASS (Assign a default management class)

Use this command to specify a management class as the default management class for a policy set. You must assign a default management class for a policy set before you can activate that policy set.

To ensure that clients can always back up and archive files, choose a default management class that contains both an archive copy group and a backup copy group.

The server uses the default management class to manage client files when a management class is not otherwise assigned or appropriate. For example, the server uses the default management class when a user does not specify a management class in the include-exclude list.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-ASsign DEFMGmtclass--domain_name--policy_set_name--class_name-><
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the management class belongs.

policy_set_name (Required)
: Specifies the policy set for which you want to assign a default management class. You cannot assign a default management class to the ACTIVE policy set.

class_name (Required)
: Specifies the management class that is to be the default management class for the policy set.

Example: Assign a default management class

Assign DEFAULT1 as the default management class for policy set SUMMER in the PROG1 policy domain.

```
assign defmgmtclass prog1 summer default1
```

Related commands

Table 1. Commands related to ASSIGN DEFMGMTCLASS

Command	Description

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE MGMTCLASS	Defines a management class.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.
QUERY POLICYSET	Displays information about policy sets.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE MGMTCLASS	Changes the attributes of a management class.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

AUDIT commands

Use the AUDIT commands to review or examine the adequacy of the database information and the storage pool volume. The AUDIT LDAPDIRECTORY command deletes nodes or administrator IDs from an LDAP directory server, that do not authenticate their passwords with the LDAP directory server.

- AUDIT CONTAINER
  - AUDIT CONTAINER (Verify the consistency of database information for a cloud container)
  - AUDIT CONTAINER (Verify the consistency of database information for a directory-container)
- AUDIT LDAPDIRECTORY (Audit an LDAP directory server)
- AUDIT LIBRARY (Audit volume inventories in an automated library)
- AUDIT LIBVOLUME (Verify database information for a tape volume)
- AUDIT LICENSES (Audit server storage usage)
- AUDIT VOLUME (Verify database information for a storage pool volume)

AIX | Linux | Windows

AUDIT CONTAINER commands

Use the AUDIT CONTAINER command to scan for inconsistencies between database information and a container in either a cloud or a directory storage pool.

- AUDIT CONTAINER (Verify the consistency of database information for a cloud container)
  Use this command to scan for inconsistencies between database information and a container in a cloud-container storage pool. Cloud-container storage pools are not supported on Linux on System z®.
- AUDIT CONTAINER (Verify the consistency of database information for a directory-container)
  Use this command to scan for inconsistencies between database information and a container in a directory-container storage pool.

AUDIT CONTAINER (Verify the consistency of database information for a cloud container)

Use this command to scan for inconsistencies between database information and a container in a cloud-container storage pool. Cloud-container storage pools are not supported on Linux on System z®.

You can use this command to complete the following actions for a container in a cloud-container storage pool:

- Scan the contents of a container to validate the integrity of the data extents

- Remove data from a container that is marked as *damaged*, such as when a file has references in the server database, but has missing or corrupted data in the cloud
- Mark an entire container as damaged
- Remove data that is marked as *orphaned*, such as when an object stored in the cloud does not have a reference in the server database

Privilege class

To use this command, you must have system privilege, or unrestricted storage privilege.

Syntax

```
>>-AUDit CONTainer--+-container_name-----------------------------------------------+-->
                    +-STGpool--=--pool_name-----------------------------------+
                    '-STGpool--=--pool_name--STGPOOLDIRectory--=--directory_name-'

   .-Action--=--SCANAll-----------.
>--+------------------------------+----------------------------->
   '-Action--=--+-SCANAll-------+-'
                +-REMOVEDamaged-+
                +-MARKDamaged---+
                '-SCANDamaged---'

   .-FORCEOrphandbdel--=--No------.
>--+------------------------------+----------------------------->
   '-FORCEOrphandbdel--=--+-No--+-'
                          '-Yes-'

   .-MAXProcess--=--4------.  .-Wait--=--No------.
>--+----------------------+--+------------------+-------------->
   '-MAXProcess--=--number-'  '-Wait--=--+-No--+-'
                                         '-Yes-'

   .-BEGINDate--=--before_first_audit-.
>--+----------------------------------+------------------------->
   '-BEGINDate--=--begin_date---------'

   .-BEGINTime--=--00:00:00---.
>--+--------------------------+-------------------------------->
   '-BEGINTime--=--begin_time-'

   .-ENDDate--=--after_last_audit-.  .-ENDTime--=--23:59:59-.
>--+-------------------------------+--+----------------------+-->
   '-ENDDate--=--end_date---------'  '-ENDTime--=--end_time-'
```

Parameters

container_name
: Specifies the name of the container that you want to audit. If you do not specify this parameter, you must specify a cloud-container storage pool.

STGpool
: Specifies the name of the cloud-container storage pool that you want to audit. This parameter is optional. If you specify only this parameter, all containers that are defined to the storage pool are audited. If you do not specify this parameter, you must specify a container.

STGPOOLDIRectory
: Specifies the name of the cloud-container storage pool directory that you want to audit. This parameter is optional. Restriction: You must specify a storage pool that uses local storage.

Action
: Specifies what action the server takes when a container in a cloud-container storage pool is audited. This parameter is optional. You can specify one of the following values:

  SCANAll
  : Specifies that the server identifies database records that refer to data extents with inconsistencies. A check is done for data in the cloud-container storage pool that does not match data in the server database. This value is the default. The server marks the data extent as damaged in the database.

Tip: If you specify the ACTION=SCANALL parameter on an IBM® Cloud Object Storage storage pool that uses a vault with name indexing disabled, the audit operation scans the entire vault to identify orphaned extents in each container. In this situation, specify WAIT=YES if you want the audit operation to wait for the scan for orphaned extents to complete before it reports the audit as complete. This scan for orphaned extents occurs only if you do not specify a container name. If you specify a container that is in a vault with name indexing disabled, the audit operation does not scan for orphaned extents.

REMOVEDamaged
: Specifies that the server removes any references to damaged extents from the server database. The damaged extents are also removed from the cloud-container storage pool if found. The server also removes any orphaned extents from the cloud-container storage pool, and removes the references to these orphaned extents from the database, as specified by the FORCEORPHANDBDEL parameter.

MARKDamaged
: Specifies that the server explicitly marks all data extents in the container as damaged.

SCANDamaged
: Specifies that the server checks only the existing damaged extents in the container.

Important: If no connection to the cloud exists, the ACTION=SCANALL and ACTION=SCANDAMAGED parameters do not run. However, the ACTION=MARKDAMAGED parameter runs as expected without a cloud connection, and the ACTION=REMOVEDAMAGED parameter marks any damaged data as orphaned. As soon as the connection to the cloud returns, the server deletes the orphaned extents.

State reset condition: If the audit does not detect an error with a data extent that is marked as damaged, the state of the data extent is reset. The data extent can then be used. This condition provides a means for resetting the state of damaged data extents if errors are caused by a correctable problem. The SCANALL and SCANDAMAGED options are the only options that reset a damaged extent if it is found not to be damaged.

FORCEOrphandbdel
: Specifies that the server forces the deletion of orphaned extents from the server database, even if they are not deleted from the cloud-container storage pool. This parameter is optional. If you specify this parameter, you must also specify the ACTION=REMOVEDAMAGED parameter. The following options are available:

Yes
: Specifies that the server deletes any orphaned extents from the server database, even if they are not deleted from the cloud-container storage pool.

No
: Specifies that the server keeps the orphaned extents in the server database if they cannot be deleted from the cloud-container storage pool. This value is the default.

MAXProcess
: Specifies the maximum number of parallel processes to use for checking a container in a cloud-container storage pool. This parameter is optional. Enter a value in the range 1 - 99. The default value is 4.

Restriction: The server ignores this parameter when you use MAXPROCESS with the ACTION=REMOVEDAMAGED parameter.

Wait
: Specifies whether the audit or verification operation is completed in the foreground or background. This parameter is optional. The following options are available:

No
: Specifies that the operation is completed in the background. You can continue with other tasks when the command is processing. Messages that are related to the background process are displayed in the activity log file or the server console, depending on where the messages are logged. This value is the default.

Yes
: Specifies that the operation is completed in the foreground. It might take a long time to complete the operation. The operation must complete before you can continue with other tasks. Messages are displayed in the activity log file or the server console, or both, depending on where the messages are logged.

Restriction: You cannot specify the WAIT=YES parameter from the server console.

BEGINDate
: Specifies the date range value at which auditing should start. Containers that were last audited within the specified date range are audited. If you specify a time but do not specify a beginning date, the current date is used. If you do not specify a beginning and end date, all containers are audited. The default is the date before the first audit was completed for the container. This parameter is optional.

You can specify the date to begin the audit in one of the following ways:

Value	Description	Example

Value	Description	Example
MM/DD/YYYY	A specific date.	09/15/2016
TODAY	The current date.	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –7 *or* –7. To audit all containers that were audited in the last week, specify BEGINDATE=TODAY-7 or BEGINDATE= -7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include containers that were audited a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include containers that were audited on the 10th day of the current month.

BEGINTime

Specifies the time range value at which auditing should start. Containers that were last audited within the specified time range are audited. If you do not specify a beginning and end time, the time range is set from 00:00:00 to 23:59:59. The default is 00:00:00. If you did not specify a date range, the default is today's date. This parameter is optional.

You can specify the date to begin the audit in one of the following ways:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date.	10:30:08
NOW	The current time on the specified begin date.	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified begin date.	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with BEGINTIME=NOW+3 or BEGINTIME=+3, containers with a last audit time of 12:00 or later on the begin date are audited.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date.	NOW-04:00 *or* -04:00. If you issue this command at 9:00 with BEGINTime=NOW-3:30 or BEGINTime= -3:30, IBM Spectrum Protect™ audits containers with a last audit time of 5:30 or later on the begin date.

ENDDate

Specifies the date range value at which auditing should stop. Containers that were last audited within the specified date range are audited. If you specify a time but do not specify a value, the current date is used. If you do not specify a beginning and end date, all containers are audited. The default is the date after the last audit was completed for the container. This parameter is optional.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date.	09/15/2016
TODAY	The current date.	TODAY

Value	Description	Example
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 *or* –1. To include containers that were audited up to yesterday, you can specify ENDDATE=TODAY-1 or ENDDATE= -1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include containers that were audited a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include containers that were audited on the 10th day of the current month.

ENDTime

Specifies the time range value at which auditing should stop. Containers that were last audited within the specified time range are audited. If you do not specify a beginning and end time, the time range is set to 00:00:00 to 23:59:59. The default is 23:59:59. This parameter is optional.

You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date.	10:30:08
NOW	The current time on the specified end date.	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date.	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with ENDTIME=NOW+3:00 or ENDTIME= +3:00, containers with a last audit time of 12:00 or earlier on the end date you specify are audited.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date.	NOW-03:30 *or* -03:30. If you issue this command at 9:00 with ENDTIME=NOW-3:30 or ENDTIME= -3:30, containers with a last audit time of 5:30 or earlier on the end date you specify are audited.

Example: Audit a specific container in a cloud-container storage pool

Audit the 42-00000my000example000container000 container in a cloud-container storage pool.

```
audit container 42-00000my000example000container000 action=scanall
```

Example: Audit a cloud-container storage pool within a specific time frame

Audit a cloud-container storage pool that is named POOL3 and only include containers from yesterday between 9:30 and 12:30.

```
audit container stgpool=pool3 begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Table 1. Commands related to AUDIT CONTAINER

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY CONTAINER	Displays information about a container.

Command	Description
QUERY DAMAGED	Displays information about damaged files.

AIX Linux Windows

AUDIT CONTAINER (Verify the consistency of database information for a directory-container)

Use this command to scan for inconsistencies between database information and a container in a directory-container storage pool.

You can use this command to complete the following actions for a container in a directory-container storage pool:

- Scan the contents of a container to validate the integrity of the data extents
- Remove damaged data from a container
- Mark an entire container as damaged

Privilege class

To issue this command, you must have system privilege, or unrestricted storage privilege.

Syntax

```
>>-AUDit CONTainer--+-container_name-----------------------------------------------+-->
                    +-STGpool--=--pool_name-----------------------------------+
                    '-STGpool--=--pool_name--STGPOOLDIRectory--=--directory_name-'

   .-Action--=--SCANAll-----------.
>--+-----------------------------+----------------------------->
   '-Action--=--+-SCANAll-------+-'
                +-REMOVEDamaged-+
                +-MARKDamaged---+
                '-SCANDamaged---'

   .-MAXProcess--=--4------.  .-Wait--=--No------.
>--+----------------------+--+------------------+-------------->
   '-MAXProcess--=--number-'  '-Wait--=--+-No--+-'
                                         '-Yes-'

   .-BEGINDate--=--before_first_audit-.
>--+-----------------------------------+------------------------>
   '-BEGINDate--=--begin_date---------'

   .-BEGINTime--=--00:00:00---.
>--+--------------------------+------------------------------->
   '-BEGINTime--=--begin_time-'

   .-ENDDate--=--after_last_audit-.  .-ENDTime--=--23:59:59-.
>--+-------------------------------+--+---------------------+--><
   '-ENDDate--=--end_date---------'  '-ENDTime--=--end_time-'
```

Parameters

container_name
: Specifies the name of the container that you want to audit. If you do not specify this parameter, you must specify a directory-container storage pool.

STGpool
: Specifies the name of the directory-container storage pool that you want to audit. This parameter is optional. If you specify only this parameter, all containers that are defined to the storage pool are audited. If you do not specify this parameter, you must specify a container.

STGPOOLDIRectory
: Specifies the name of the container storage pool directory that you want to audit. This parameter is optional. If you specify this parameter, all containers that are defined to the container storage pool directory are audited. To specify this parameter,

you must also specify a storage pool.

Action

Specifies what action the server takes when a container in a directory-container storage pool is audited. This parameter is optional. You can specify one of the following values:

SCANAll
: Specifies that the server identifies database records that refer to data extents with inconsistencies. This value is the default. The server marks the data extent as damaged in the database.
Tip: If you used the PROTECT STGPOOL command on a directory-container storage pool on the target server, you can repair the damaged data extent by using the REPAIR STGPOOL command.

REMOVEDamaged
: Specifies that the server removes any files from the database that reference the damaged data extent.

MARKDamaged
: Specifies that the server explicitly marks all data extents in the container as damaged.

SCANDamaged
: Specifies that the server checks only the existing damaged extents in the container.

State reset condition: If the audit does not detect an error with a data extent that is marked as damaged, the state of the data extent is reset. The data extent can then be used. This condition provides a means for resetting the state of damaged data extents if errors are caused by a correctable problem. The SCANALL and SCANDAMAGED options are the only options that reset a damaged extent if it is found not to be damaged.

MAXProcess

Specifies the maximum number of parallel processes to use for checking a container in a directory-container storage pool. This parameter is optional. Enter a value in the range 1 - 99. The default value is 4.

Wait

Specifies whether the audit or verification operation is completed in the foreground or background. This parameter is optional. The following options are available:

No
: Specifies that the operation is completed in the background. You can continue with other tasks when the command is processing. Messages that are related to the background process are displayed in the activity log file or the server console, depending on where the messages are logged. This is the default value.

Yes
: Specifies that the operation is completed in the foreground. It might take a long time to complete the operation. The operation must complete before you can continue with other tasks. Messages are displayed in the activity log file or the server console, or both, depending on where the messages are logged.
Restriction: You cannot specify the WAIT=YES parameter from the server console.

BEGINDate

Specifies the date range value at which auditing should start. Containers that were last audited within the specified date range are audited. If you specify a time but do not specify a beginning date, the current date is used. If you do not specify a beginning and end date, all containers are audited. The default is the date before the first audit was completed for the container. This parameter is optional.
You can specify the date to begin the audit in one of the following ways:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date.	09/15/2016
TODAY	The current date.	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –7 *or* –7. To audit all containers that were audited in the last week, specify BEGINDATE=TODAY-7 or BEGINDATE= -7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include containers that were audited a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include containers that were audited on the 10th day of the current month.

BEGINTime

Specifies the time range value at which auditing should start. Containers that were last audited within the specified time range are audited. If you do not specify a beginning and end time, the time range is set from 00:00:00 to 23:59:59. The default is 00:00:00. If you did not specify a date range, the default is today's date. This parameter is optional.

You can specify the date to begin the audit in one of the following ways:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date.	10:30:08
NOW	The current time on the specified begin date.	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified begin date.	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with BEGINTIME=NOW+3 or BEGINTIME=+3, containers with a last audit time of 12:00 or later on the begin date are audited.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date.	NOW-04:00 *or* -04:00. If you issue this command at 9:00 with BEGINTime=NOW-3:30 or BEGINTime= -3:30, IBM Spectrum Protect™ audits containers with a last audit time of 5:30 or later on the begin date.

ENDDate

Specifies the date range value at which auditing should stop. Containers that were last audited within the specified date range are audited. If you specify a time but do not specify a value, the current date is used. If you do not specify a beginning and end date, all containers are audited. The default is the date after the last audit was completed for the container. This parameter is optional.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date.	09/15/2016
TODAY	The current date.	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 *or* –1. To include containers that were audited up to yesterday, you can specify ENDDATE=TODAY-1 or ENDDATE= -1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include containers that were audited a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include containers that were audited on the 10th day of the current month.

ENDTime

Specifies the time range value at which auditing should stop. Containers that were last audited within the specified time range are audited. If you do not specify a beginning and end time, the time range is set to 00:00:00 to 23:59:59. The

default is 23:59:59. This parameter is optional.
You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date.	10:30:08
NOW	The current time on the specified end date.	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date.	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with ENDTIME=NOW+3:00 or ENDTIME= +3:00, containers with a last audit time of 12:00 or earlier on the end date you specify are audited.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date.	NOW-03:30 *or* -03:30. If you issue this command at 9:00 with ENDTIME=NOW-3:30 or ENDTIME= -3:30, containers with a last audit time of 5:30 or earlier on the end date you specify are audited.

Example: Audit a specific storage pool container

Audit the 0000000000000721.dcf storage pool container.

```
audit container n:\ddcont2\07\0000000000000721.dcf action=scanall
```

Example: Remove damaged data from a directory-container storage pool

Audit a directory-container storage pool that is named NEWDEDUP and remove damaged files.

```
audit container stgpool=newdedup action=removedamaged
```

Example: Mark as damaged all of the data in a directory-container storage pool

Audit a directory-container storage pool that is named NEWDEDUP and mark all files as damaged.

```
audit container stgpool=newdedup maxprocess=2 action=markdamaged
```

Example: Audit a directory-container storage pool within a specific time frame

Audit a directory-container storage pool that is named POOL2 and only include containers before yesterday between 9:30 and 12:30.

```
audit container stgpool=pool2 begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Table 1. Commands related to AUDIT CONTAINER

Command	Description
CANCEL PROCESS	Cancels a background server process.
MOVE CONTAINER	Moves the contents of a storage pool container to another container.
QUERY DAMAGED	Displays information about damaged files.

AUDIT LDAPDIRECTORY (Audit an LDAP directory server)

Use this command to audit an IBM Spectrum Protect™ controlled namespace on a Lightweight Directory Access Protocol (LDAP) server. The LDAP server and namespace are specified by using one or more LDAPURL options.

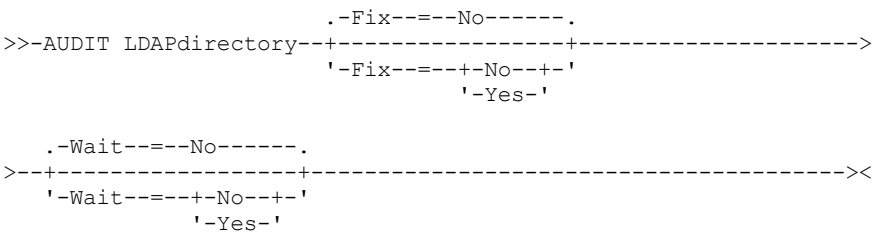
Restriction: Use this command only if you configured password authentication as described in Authenticating users by using an LDAP server. Information that is provided about the AUDIT LDAPDIRECTORY command applies only to environments in which

password authentication is configured as described in Authenticating users by using an LDAP server.
Nodes and administrator user IDs that do not authenticate their passwords with the LDAP directory server are deleted with the AUDIT LDAPDIRECTORY FIX=YES command. Nodes or administrator user IDs that no longer exist in the IBM Spectrum Protect database are also deleted.
Before you issue this command, ensure that the LDAPURL option is specified in the dsmserv.opt file. See the LDAPURL option for more information. If you specified more than one LDAPURL option in the dsmserv.opt file, each option is validated in the order in which they are placed. If the LDAPURL option is not specified, the command fails.

Privilege class

You must have system privileges to issue this command.

Syntax



Parameters

Fix
: This optional parameter specifies how the IBM Spectrum Protect server resolves inconsistencies between the database and the external directory. The default is NO. You can specify the following values:

  No
  : The server reports all inconsistencies but does not change the external directory.

  Yes
  : The server resolves any inconsistencies that it can and suggests further actions, if needed.
  Important: If there are LDAP entries that are shared with other IBM Spectrum Protect servers, choosing YES might cause those servers to become out-of-sync.

Wait
: This optional parameter specifies whether to wait for the IBM Spectrum Protect server to complete processing this command in the foreground. The default is NO. You can specify the following values:

  No
  : The server processes this command in the background and you can continue with other tasks while the command is processing. Messages related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged.

  Yes
  : The server processes this command in the foreground. The operation must complete before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.
  Restriction: You cannot specify WAIT=YES from the server console.

Example: Audit an LDAP directory and repair inconsistencies

Audit the LDAP directory that you specified in the LDAPURL option. The IBM Spectrum Protect server resolves some inconsistencies.

```
audit ldapdirectory fix=yes


ANR2749W Admin ADMIN1 was located in the LDAP directory server but not
in the database.
ANR2749W Admin ADMIN2 was located in the LDAP directory server but not
in the database.
```

```
ANR2749W Admin NODE1 was located in the LDAP directory server but not
in the database.
ANR2749W Admin NODE2 was located in the LDAP directory server but not
in the database.
ANR2748W Node NODE1 was located in the LDAP directory server but not
in the database.
ANR2748W Node NODE2 was located in the LDAP directory server but not
in the database.
ANR2745I AUDIT LDAPDIRECTORY command completed: 4 administrator
entries are only in the LDAP directory server (not in the IBM Spectrum
Protect server), 0 administrator entries are only in the IBM Spectrum
Protect server (not in the LDAP directory server), 2 node entries are
only in the LDAP directory server (not in the IBM Spectrum Protect
server), 0 node entries are only in the IBM Spectrum Protect server,
(not in the LDAP directory server), 6 entries were deleted from the
LDAP server in total.
```

Related commands

Table 1. Commands related to AUDIT LDAPDIRECTORY

Command	Description
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET LDAPPASSWORD	Sets the password for the LDAPUSER.
SET LDAPUSER	Sets the user who oversees the passwords and administrators on the LDAP directory server.

AUDIT LIBRARY (Audit volume inventories in an automated library)

Use this command to audit and synchronize volume inventories in an automated library.

When the AUDIT LIBRARY command is issued on a library client, the client synchronizes its inventory with the inventory on the library manager. If the library client detects inconsistencies, it corrects them by changing the ownership of the volume on the library manager.

When the AUDIT LIBRARY command is issued on a server where the library is SCSI, 349X, or ACSLS (LIBTYPE=SCSI, LIBTYPE=349X, or LIBTYPE=ACSLS), the server synchronizes its inventory with the inventory of the library device. If the server detects inconsistencies, it deletes missing volumes from its inventory.

- In SCSI libraries, the server also updates the locations of volumes in its inventory that have been moved since the last audit.
- In 349X libraries, the server also ensures that scratch volumes are in the scratch category and that private volumes are in the private category.

When the AUDIT LIBRARY command is issued on a server that is a library manager for the library (SHARED=YES), the server updates ownership of its volumes if it detects inconsistencies.

Regardless the type of server or type of library, issuing the AUDIT LIBRARY command does not automatically add new volumes to a library. To add new volumes, you must use the CHECKIN LIBVOLUME command.

Attention: The following precautions apply to SCSI, 349X, and ACSLS libraries only (LIBTYPE=SCSI, LIBTYPE=349X, and LIBTYPE=ACSLS):

- Running the AUDIT LIBRARY command prevents any other library activity until the audit completes. For example, the server will not process restore or retrieve requests that involve the library when the AUDIT LIBRARY command is running.
- If other activity is occurring in the library, do not issue the AUDIT LIBRARY command. Issuing the AUDIT LIBRARY command when a library is active can produce unpredictable results (for example, a hang condition) if a process currently accessing the library attempts to acquire a new tape mount.

This command creates a background process that you can cancel with the CANCEL PROCESS command. To display information about background processes, use the QUERY PROCESS command.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-AUDIT LIBRary--library_name---------------------------------->

   .-CHECKLabel--=--Yes---------.
>--+----------------------------+------------------------------->
   '-CHECKLabel--=--+-Yes-----+-'
                    '-Barcode-'

   .-REFRESHstate--=--No------.
>--+-------------------------+------------------------------><
   '-REFRESHstate--=--+-No--+-'
                      '-Yes-'
```

Parameters

library_name (Required)
: Specifies the name of the library to audit.

CHECKLabel
: Specifies how the storage volume label is checked during the audit. This parameter applies to SCSI libraries only. The parameter is ignored for other library types. The default is YES. Possible values are:

  Yes
  : Specifies that the server checks each volume label to verify the identity of the volume.

  Barcode
  : Specifies that the server uses the barcode reader to read the storage label. Using the barcode decreases the audit processing time. This parameter applies only to SCSI libraries.
    Attention: If the scanner cannot read the barcode label or the barcode label is missing, the server loads that tape in a drive to read the label.

REFRESHstate
: Specifies whether the server's information about a library, which is normally obtained during initialization, is refreshed, so that any changes in configuration are reflected. By setting the REFRESHSTATE parameter to Yes, this action is completed without having to restart the server or re-define the library. The default is No. Possible values are:

  No
  : Specifies that the server does not refresh the library's state when the library is audited.

  Yes
  : Specifies that the server does refresh the library's state when the AUDIT LIBRARY command is issued.

Example: Audit an automated library

Audit the EZLIFE automated library.

```
audit library ezlife
```

Related commands

Table 1. Commands related to AUDIT LIBRARY

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE LIBRARY	Deletes a library.
DISMOUNT VOLUME	Dismounts a sequential, removable volume by the volume name.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.

Command	Description
QUERY PROCESS	Displays information about background processes.
UPDATE LIBRARY	Changes the attributes of a library.

AUDIT LIBVOLUME (Verify database information for a tape volume)

Use this command to determine whether a tape volume is intact and to audit data on any tape volume.

You can issue the AUDIT LIBVOLUME command from any tape volume that is checked in to a library. The command runs in the background by default. You can issue the command from the following library types that have IBM® TS1140, IBM LTO 5, or a later generation tape drive:

- SCSI tape library
- Virtual tape library (VTL)

The following table outlines the tape drives that can verify tape volumes with media types for IBM TS1140 and IBM LTO 5 and later generation LTO tape drives:

Table 1. Tape drives and the media types

Drive	Media type
TS1140	JB, JX, JA, JW, JJ, JR, JC, JY, and JK
IBM LTO 5	LTO 3, LTO 4, and LTO 5
IBM LTO 6	LTO 4, LTO 5, and LTO 6
IBM LTO 7	LTO 5, LTO 6, and LTO 7

The following table outlines the minimum device driver level that you require to run the command:

Table 2. Minimum IBM device driver level

Driver name	Device driver level
Atape driver on AIX®	12.3.5.00
lin_tape driver on Linux	1.6.7.00
IBM tape driver on Windows	6.2.2.00

Restriction: You cannot issue the CANCEL PROCESS command while the AUDIT LIBVOLUME command is in progress.

Privilege class

To issue this command, you must have system privilege, or unrestricted storage privilege for the library to which the tape volume is defined.

Syntax

```
>>-AUDit LIBVolume--library_name--volume_name------------------->

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameters

library_name (Required)
: Specifies the name of the library volume where the tape volume is located that you want to audit.

volume_name (Required)
: Specifies the name of the physical tape volume that you want to audit.

Wait (Optional)
: Specifies whether the audit or verification operation is completed in the foreground or background. This parameter is optional. The following options are available:

No
: Specifies that the operation is completed in the background. The NO value is the default value.

Yes
: Specifies that the operation is completed in the foreground. It might take a long time to complete the operation.

Example: Audit a tape volume

Audit the EZLIFE library that has a tape volume that is called KM0347L5.

```
audit libvolume ezlife KM0347L5
```

AUDIT LICENSES (Audit server storage usage)

Use this command to audit the server storage used by client nodes and to audit the server licenses. The audit determines whether the current configuration is in compliance with the license terms.

An audit creates a background process you can cancel with the CANCEL PROCESS command. If you halt and restart the server, an audit is run automatically as specified by the SET LICENSEAUDITPERIOD. To view audit results, use the QUERY LICENSE command.

Attention: The audit of server storage can take a lot of CPU time. You can use the AUDITSTORAGE server option to specify that storage is not to be audited.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-AUDit LICenses-----------------------------------------><
```

Parameters

None.

Example: Audit server licenses

Issue the AUDIT LICENSES command.

```
audit licenses
```

Related commands

Table 1. Commands related to AUDIT LICENSES

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY AUDITOCCUPANCY	Displays the server storage utilization for a client node.
QUERY LICENSE	Displays information about licenses and audits.
QUERY PROCESS	Displays information about background processes.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER LICENSE	Registers a license with the IBM Spectrum Protect server.
SET LICENSEAUDITPERIOD	Specifies the number of days between automatic license audits.

AUDIT VOLUME (Verify database information for a storage pool volume)

Use this command to check for inconsistencies between database information and a storage pool volume. Processing information generated during an audit is sent to the activity log and server console.

Restriction: You cannot use this command for volumes that are assigned to copy-container storage pools.
You can only audit volumes that belong to storage pools with DATAFORMAT=NATIVE and DATAFORMAT=NONBLOCK.

You cannot audit a volume if it is being deleted from a primary or copy storage pool.

While an audit process is active, clients cannot restore data from the specified volume or store new data to that volume.

If the server detects a file with errors, handling of the file will depend on the type of storage pool to which the volume belongs, whether the FIX option is specified on this command, and whether the file is also stored on a volume assigned to other pools.

If IBM Spectrum Protect™ does not detect errors for a file that was marked as damaged, the state of the file is reset so that it can be used.

The server will not delete archive files that are on deletion hold. If archive retention protection is enabled, the server will not delete archive files whose retention period has not expired.

To display information about the contents of a storage pool volume, use the QUERY CONTENT command.

To audit multiple volumes, you can use the FROMDATE and TODATE parameters. Use the STGPOOL parameter to audit all volumes in a storage pool. When you use the parameters FROMDATE, TODATE, or both, the server limits the audit to only the sequential media volumes that meet the date criteria, and automatically includes all online disk volumes in storage. To limit the number of volumes that may include disk volumes, use the FROMDATE, TODATE, and STGPOOL parameters.

If you are running a server with archive retention protection enabled, and you have data stored in storage pools which are defined with the parameter RECLAMATIONTYPE=SNAPLOCK, the Last Access Date on the NetApp SnapLock Filer for a volume should be equal to the End Reclaim Period date that you see when you issue a QUERY VOLUME F=D command on that volume. During AUDIT VOLUME processing, these dates are compared. If they do not match and the AUDIT VOLUME command is being run with the FIX=NO parameter, a message will be issued to you indicating that the command should be run with the FIX=YES parameter to resolve the inconsistency. If they do not match and the AUDIT VOLUME command is being run with the FIX=YES parameter, the inconsistencies will be resolved.

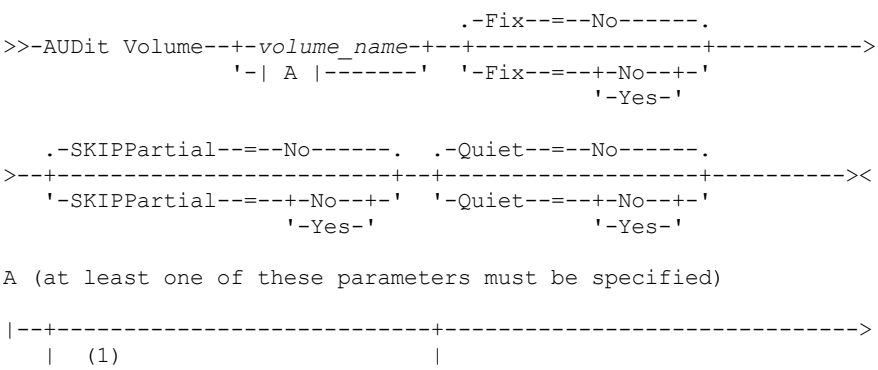
Attention: Use the FIX=Yes parameter only if your tape drive and storage area network (SAN) infrastructure is stable. Ensure that the tape heads are clean and that the tape device drivers are stable and reliable. Otherwise, you risk deleting data that is error free when you use this parameter. The server cannot determine whether a tape is physically damaged or whether a tape infrastructure is unstable.

This command creates a background process that can be canceled with the CANCEL PROCESS command. To display information on background processes, use the QUERY PROCESS command.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to which the volume is defined.

Syntax



```
   '-------STGPool--=--poolname-'

      (1)                                          (1)
   .-------FROMDate--=--TODAY-.   .-TODate--=--TODay-----.
>--+------------------------+--+---------------------+-------|
   '-FROMDate--=-----date------'   '-TODate--=-----date----'
```

Notes:

1. You cannot specify a volume name if you specify a storage pool name, FROMDATE, or TODATE.

Parameters

volume_name
: Specifies the name of the storage pool volume you want to audit. This parameter is required if you do not specify a storage pool. You cannot specify a volume name together with the FROMDATE and TODATE parameters.

Fix
: Specifies how the server resolves inconsistencies between the database inventory and the specified storage pool volume. This parameter is optional. The default is NO.

  The actions the server performs depend on whether the volume is assigned to a primary or a copy storage pool.

  Primary Storage Pool:

  Note: If the AUDIT VOLUME command does not detect an error in a file that was previously marked as damaged, IBM Spectrum Protect resets the state of the file so that it can be used. This provides a means for resetting the state of damaged files if it is determined that the errors were caused by a correctable hardware problem such as a dirty tape head.

  Fix=No
  : IBM Spectrum Protect reports, but does not delete, database records that refer to files with inconsistencies:

    - IBM Spectrum Protect marks the file as damaged in the database. If a backup copy is stored in a copy storage pool, you can restore the file using the RESTORE VOLUME or RESTORE STGPOOL command.
    - If the file is a cached copy, you must delete references to the file on this volume by issuing the AUDIT VOLUME command and specifying FIX=YES. If the physical file is not a cached copy, and a duplicate is stored in a copy storage pool, it can be restored by using the RESTORE VOLUME or RESTORE STGPOOL command.

  Fix=Yes
  : The server fixes any inconsistencies as they are detected:

    - If the physical file is a cached copy, the server deletes the database records that refer to the cached file. The primary file is stored on another volume.
    - If the physical file is not a cached copy, and the file is also stored in one or more copy storage pools, the error will be reported and the physical file marked as damaged in the database. You can restore the physical file by using the RESTORE VOLUME or RESTORE STGPOOL command.
    - If the physical file is not a cached copy, and the physical file is not stored in a copy storage pool, each logical file for which inconsistencies are detected are deleted from the database.
    - If archive retention protection is enabled by using the SET ARCHIVERETENTIONPROTECTION command, a cached copy of data can be deleted if needed. Data in primary and copy storage pools can only be marked damaged and never deleted.

    Do not use the AUDIT VOLUME command with FIX=YES if a restore process (RESTORE STGPOOL or RESTORE VOLUME) is running. The AUDIT VOLUME command could cause the restore to be incomplete.

  Copy Storage Pool:

  Fix=No
  : The server reports the error and marks the physical file copy as damaged in the database.

  Fix=Yes
  : The server deletes any references to the physical file and any database records that point to a physical file that does not exist.

SKIPPartial
: Specifies whether IBM Spectrum Protect ignores partial files, which are files that span multiple storage pool volumes. This parameter is optional. The default value is NO. When performing an audit operation on a sequential access media volume,

this parameter prevents additional sequential access media mounts that may be necessary to audit any partial files. Possible values are:

No
: IBM Spectrum Protect audits files that span multiple volumes.
Unless you specify SKIPPARTIAL=YES, IBM Spectrum Protect attempts to process each file stored on the volume, including files that span into and out of other volumes. To audit files that span multiple volumes, the following conditions must be true:

- For sequential access volumes, the additional sequential access volumes must have an access mode of read/write or read-only.
- For random access volumes, the additional volumes must be online.

Yes
: IBM Spectrum Protect audits only files that are stored on the volume to be audited. The status of any partial files is unknown.

Quiet
: Specifies whether IBM Spectrum Protect sends detailed informational messages to the activity log and the server console about irretrievable files on the volume. This parameter is optional. The default is NO. Possible values are:

No
: Specifies that IBM Spectrum Protect sends detailed informational messages and a summary. Each message contains the node, file space, and client name for the file.

Yes
: Specifies that IBM Spectrum Protect sends only a summary report.

FROMDate
: Specifies the beginning date of the range to audit volumes. The default is the current date. All sequential media volumes meeting the time range criteria that were written to after this date are audited. The server includes all online disk volumes in storage. The server starts one audit process for each volume and runs the process serially. You cannot use this parameter if you have specified a volume. This parameter is optional. To limit the number of volumes that may include disk volumes, use the FROMDATE, TODATE, and STGPOOL parameters.
You can specify the date by using one of the following values:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	10/15/2001 If a date is entered, all candidate volumes written on that day (starting at 12:00:01 am) will be evaluated.
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –7 *or* –7. To display information beginning with volumes written a week ago, you can specify FROMDATE=TODAY-7 or FROMDATE= -7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

TODate

Specifies the ending date of the range for volumes to audit. All sequential media volumes meeting the time range criteria that were written to before this date are audited. The server includes all online disk volumes in storage. If you do not specify a value, the server defaults to the current date. You cannot use this parameter if you have specified a volume. This parameter is optional. To limit the number of volumes that may include disk volumes, use the FROMDATE, TODATE, and STGPOOL parameters.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	10/15/2001 If a date is entered, all candidate volumes written on that day (ending at 11:59:59 pm) will be evaluated.
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 **or** –1. To display information created up to yesterday, you can specify TODATE=TODAY-1 or simply TODATE=-1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

STGPool

This parameter specifies that the server only audits the volumes from the specified storage pool. This parameter is optional. You cannot use this parameter if you have specified a volume.

Example: Verify database information for a specific storage pool volume

Verify that the database information for storage pool volume PROG2 is consistent with the data stored on the volume. IBM Spectrum Protect fixes any inconsistencies.

```
audit volume prog2 fix=yes
```

Example: Verify database information for all volumes written to during a specific date range

Verify that the database information for all eligible volumes written to from 3/20/2002 to 3/22/2002 is consistent with data stored on the volume.

```
audit volume fromdate=03/20/2002 todate=03/22/2002
```

Example: Verify database information for all volumes in a specific storage pool

Verify that the database information for all volumes in storage pool STPOOL3 is consistent with data stored on the volume for today.

```
audit volume stgpool=STPOOL3
```

Example: Verify database information for all volumes in a specific storage pool written to in the last two days

Verify that the database information for all volumes in storage pool STPOOL3 is consistent with data stored on the volume for the last two days.

```
audit volume stgpool=STPOOL3 fromdate=-1
```

Related commands

Table 1. Commands related to AUDIT VOLUME

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY PROCESS	Displays information about background processes.
QUERY VOLUME	Displays information about storage pool volumes.
SET ARCHIVERETENTIONPROTECTION	Specifies whether data retention protection is activated.

BACKUP commands

Use the BACKUP commands to create backup copies of IBM Spectrum Protect™ information or objects.

- BACKUP DB (Back up the database)
- BACKUP DEVCONFIG (Create backup copies of device configuration information)
- BACKUP NODE (Back up a NAS node)
- BACKUP STGPOOL (Back up primary storage pool data to a copy storage pool)
- BACKUP VOLHISTORY (Save sequential volume history information)

BACKUP DB (Back up the database)

Use this command to back up an IBM Spectrum Protect™ database to sequential access volumes.

Attention: To restore a database, the server must use information from the volume history file and the device configuration file. You must make and save copies of the volume history file and the device configuration file. These files cannot be recreated.

To determine how much extra storage space a backup requires, issue the QUERY DB command.

Restrictions: You cannot restore a server database if the release level of the server database backup is different from the release level of the server that is being restored. For example, an error occurs when you restore a Version 6.3 database and you are using a Version 7.1 server.
After the database backup is complete, the IBM Spectrum Protect server backs up information, depending on the options that are specified in the server options file. The following information is backed up:

- Sequential volume-history information is backed up to all files that the VOLUMEHISTORY option specifies
- Information about device configuration is backed up to all files that the DEVCONFIG option specifies
- The server's master encryption key

If there is not enough space available on the defined active log directory volume or file space, you can define the DB2® option, *overflowlogpath*, to use a directory with the required space available. For example, use the following command to use the /home/tsminst2/overflow_dir directory:

```
db2 update db cfg for TSMDB1 using overflowlogpath /home/tsminst2/overflow_dir
```

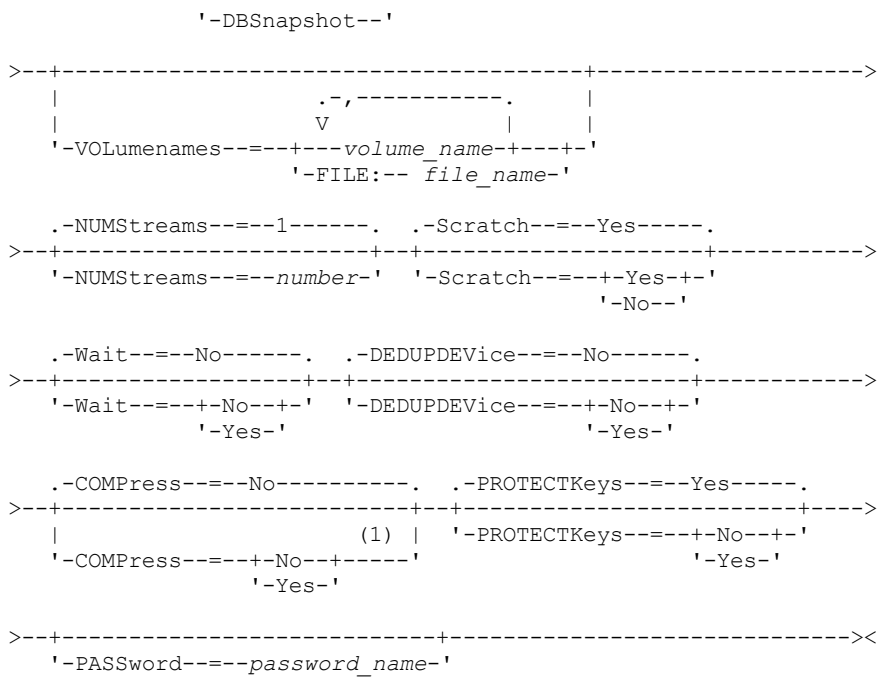
Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-BAckup DB--DEVclass--=--device_class_name--------------------->

   .-Type--=--Full------------.
>--+--------------------------+-------------------------------->
   '-Type--=--+-Incremental-+-'
              +-Full--------+
```



Notes:

1. The default value of the COMPRESS parameter is conditional. If you specify the COMPRESS parameter in the BACKUP DB command, it overrides any COMPRESS parameter value that is set in the SET DBRECOVERY command. Otherwise, the value that is set in the SET DBRECOVERY command is the default.

Parameters

DEVclass (Required)
: Specifies the name of the sequential access device class to use for the backup. If you issue the BACKUP DB command, and the device class is not the one that is specified in the SET DBRECOVERY command, a warning message is issued. However, the backup operation continues and is not affected.

  If the SET DBRECOVERY command is not issued to set a device class, the BACKUP DB command fails.

  Restriction:

  - You cannot use a device class with a device type of NAS or CENTERA.
  - A restore database operation fails if the source for the restore is a FILE library. A FILE library is created if the FILE device class specifies SHARED=YES.

  If all drives for this device class are busy when the backup runs, IBM Spectrum Protect cancels lower priority operations, such as reclamation, to make a drive available for the backup.

Type
: Specifies the type of backup to run. This parameter is optional. The default is FULL. The following values are possible:

  Full
  : Specifies that you want to run a full backup of the IBM Spectrum Protect database.

  Incremental
  : Specifies that you want to run an incremental backup of the IBM Spectrum Protect database. An incremental (or cumulative) backup image contains a copy of all database data that is changed since the last successful full backup operation.

  DBSnapshot
  : Specifies that you want to run a full snapshot database backup. The entire contents of a database are copied and a new snapshot database backup is created without interrupting the existing full and incremental backup series for the database.

VOLumenames

Specifies the volumes that are used to back up the database. This parameter is optional. However, if you specify SCRATCH=NO, you must specify a list of volumes.

volume_name
: Specifies the volumes that are used to back up the database. Specify multiple volumes by separating the names with commas and no intervening spaces.

FILE:filename
: Specifies the name of a file that contains a list of volumes that are used to back up the database. Each volume name must be on a separate line. Blank lines and comment lines, which begin with an asterisk, are ignored.
For example, to use volumes DB0001, DB0002, and DB0003, create a file that contains these lines:

```
DB0001
DB0002
DB0003
```

Name the file appropriately. For example:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

You can then specify the volumes for the command as follows:

AIX Linux

```
VOLUMENAMES=FILE:TAPEVOL
```

Windows

```
VOLUMENAMES=FILE:TAPEVOL.DATA
```

NUMStreams
: Specifies the number of parallel data movement streams to use when you back up the database. The minimum value is 1, and the maximum value is 32. Increasing the value causes a corresponding increase in the number of database backup sessions to be used and the number of drives to be used for the device class. If you specify a NUMSTREAMS value in the BACKUP DB command, it overrides any value that is set in the SET DBRECOVERY command. Otherwise, the value that is set in the SET DBRECOVERY command is used. The NUMSTREAMS value is used for all types of database backups.
If a value is specified that is greater than the number of drives available for the device class, only the number of available drives are used. The available drives are those defined to the device class by the MOUNTLIMIT parameter or by the number of online drives for the specified device class. The session is displayed in the QUERY SESSION output.
If you increase the number of streams, more volumes are used from the corresponding device class for this operation. Using more volumes might improve the speed of the database backups, but at the cost of more volumes that are not fully used.

Scratch
: Specifies whether scratch volumes can be used for the backup. This parameter is optional. The default is YES. The following values are possible:

Yes
: Specifies that scratch volumes can be used.

If you specify SCRATCH=YES and the VOLUMENAMES parameter, IBM Spectrum Protect uses only scratch volumes if space is unavailable on the specified volumes.

If you do not include a list of volumes by using the VOLUMENAMES parameter, you must either specify SCRATCH=YES or use the default.

No
: Specifies that scratch volumes cannot be used.

If you specify volumes by using the VOLUMENAMES parameter and SCRATCH=NO, the backup fails if there is not enough space available to store the backup data on the specified volumes.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. The default is NO. The following values are possible:

No
: Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If a BACKUP DB background process is canceled, some of the database might have already been backed up before the cancellation.

Yes

Specifies that the server processes this command in the foreground. Wait for the command to complete before you continue with other tasks. The server then displays the output messages to the administrative client when the command completes.
Restriction: You cannot specify WAIT=YES from the server console.

DEDUPDEVice

Specifies that a target storage device supports data deduplication. When set to YES, the format for backup images is optimized for data deduplication devices, making backup operations more efficient. The following values are possible:

No

Specifies that a target storage device does not support data deduplication. NO is the default.
Ensure that this parameter is set to NO for the following devices:

- SCSI libraries
- All devices that are defined with a FILE device class
- Virtual tape libraries (VTL) that do not support the data deduplication function

Yes

Specifies that a target device supports data deduplication and that you want to optimize backups for this function. You can set this parameter to YES if you are using VTLs that support data deduplication.

COMPress

Specifies whether volumes that are created by the BACKUP DB command are compressed. The COMPRESS value is used for all types of database backups. This parameter is optional. The default value is conditional. If you specify the COMPRESS parameter on the BACKUP DB command, it overrides any value that is set in the SET DBRECOVERY command. Otherwise, the value that is set in the SET DBRECOVERY command is the default. You can specify one of the following values:

No

Specifies that the volumes that are created by the BACKUP DB command are not compressed.

Yes

Specifies that the volumes that are created by the BACKUP DB command are compressed.

Restrictions:

- Use caution when you specify the COMPRESS parameter. Using compression during database backups can reduce the size of the backup files. However, compression can increase the time that is required to complete database backup processing.
- Do not back up compressed data to tape. If your system environment stores database backups on tape, set the COMPRESS parameter to No in the SET DBRECOVERY and BACKUP DB commands.

AIX | Linux | Windows PROTECTKeys

AIX | Linux | Windows Specifies that database backups include a copy of the server master encryption key that is used to encrypt node passwords, administrator passwords, and storage pool data. The master encryption key is stored in the dsmkeydb files. If you lose the dsmkeydb files, nodes and administrators are unable to authenticate with the server because the server is unable to read the passwords that are encrypted by using the master encryption key. In addition, any data that is stored in an encrypted storage pool cannot be retrieved without the master encryption key. This parameter is optional. The default is the value that is specified for the PROTECTKEYS parameter on the SET DBRECOVERY command. You can specify one of the following values:

No

Specifies that database backups do not include a copy of the server master encryption key.
Attention: If you specify PROTECTKEYS=NO, you must manually back up the master encryption key for the server and make the key available when you implement disaster recovery. You cannot recover from a disaster without the master encryption key.

Yes

Specifies that database backups include a copy of the server master encryption key.

Attention: If you specify PROTECTKEYS=YES, you must also specify the PASSWORD parameter.

AIX Linux Windows PASSword

AIX Linux Windows Specifies the password that is used to protect the database backup. The default is the value that is specified for the PASSWORD parameter on the SET DBRECOVERY command. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.
Important: Ensure that you remember this password. If you specify a password for database backups, you must specify the same password on the RESTORE DB command to restore the database.

Example: Run an incremental backup by using a scratch volume

Run an incremental backup of the database by using a scratch volume. Use a device class of FILE for the backup.

```
backup db devclass=file type=incremental
```

AIX Linux Windows

Example: Encrypt storage pool data in database backups

Encrypt storage pool data by specifying that database backups include a copy of the server master encryption key. Issue the following command:

```
backup db protectkeys=yes password=password_name
```

Related commands

Table 1. Commands related to BACKUP DB

Command	Description
BACKUP DEVCONFIG	Backs up IBM Spectrum Protect device information to a file.
BACKUP VOLHISTORY	Records volume history information in external files.
CANCEL PROCESS	Cancels a background server process.
DELETE VOLHISTORY	Removes sequential volume history information from the volume history file.
EXPIRE INVENTORY	Manually starts inventory expiration processing.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
PREPARE	Creates a recovery plan file.
QUERY DB	Displays allocation information about the database.
QUERY PROCESS	Displays information about background processes.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
SET DBRECOVERY	Specifies the device class to be used for automatic backups.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.

BACKUP DEVCONFIG (Create backup copies of device configuration information)

Use this command to back up information about device configuration for the server.

Attention: To restore a database, the server must use information from the volume history file and the device configuration file. You must make and save copies of the volume history file and the device configuration file. These files cannot be recreated. This command backs up the following information in one or more files:

- Device class definitions
- Library definitions

- Drive definitions
- Path definitions when SRCTYPE=SERVER
- Server definitions
- Server name
- Server password
- Volume location information for LIBTYPE=SCSI libraries

AIX Linux You can use the DEVCONFIG server option to specify one or more files in which to store device configuration information. IBM Spectrum Protect™ updates the files whenever a device class, library, or drive is defined, updated, or deleted.

Windows At installation, the server options file includes a DEVCONFIG option that specifies a device configuration file named devcnfg.out. IBM Spectrum Protect updates this file whenever a device class, library, or drive is defined, updated, or deleted.

To ensure updates are complete before the server is halted:

- Do not halt the server for a few minutes after issuing the BACKUP DEVCONFIG command.
- Specify multiple DEVCONFIG options in the server options file.
- Examine the device configuration file to see if the file has been updated.

Privilege class

Any administrator can issue this command unless it includes the FILENAMES parameter. If the FILENAMES parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES, the administrator must have system privilege. If the FILENAMES parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have operator, policy, storage or system privilege.

Syntax

```
>>-BAckup DEVCONFig--+---------------------------------+--------><
                     |               .-,------------.  |
                     |               V              |  |
                     '-Filenames--=------filename---+-'
```

Parameters

Filenames
: Specifies the files in which to store device configuration information. You can specify multiple files by separating the names with commas and no intervening spaces. This parameter is optional.

  If you do not specify a file name, IBM Spectrum Protect stores the information in all files specified with the DEVCONFIG option in the server options file.

Example: Backup device configuration information to a file

Back up device configuration information to a file named DEVICE.

```
backup devconfig filenames=device
```

Related commands

Table 1. Commands related to BACKUP DEVCONFIG

Command	Description
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE DEVCLASS	Defines a device class.
AIX Linux DEFINE DEVCLASS (z/OS® media server)	AIX Linux Defines a device class to use storage managed by a z/OS media server.
DEFINE DRIVE	Assigns a drive to a library.

Command	Description
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DEFINE SERVER	Defines a server for server-to-server communications.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
QUERY LIBVOLUME	Displays information about a library volume.
SET SERVERNAME	Specifies the name by which the server is identified.
SET SERVERPASSWORD	Specifies the server password.
UPDATE DEVCLASS	Changes the attributes of a device class.
AIX Linux UPDATE DEVCLASS (z/OS media server)	AIX Linux Changes the attributes of a device class for storage managed by a z/OS media server.
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE LIBRARY	Changes the attributes of a library.
UPDATE LIBVOLUME	Changes the status of a storage volume.
UPDATE PATH	Changes the attributes associated with a path.
UPDATE SERVER	Updates information about a server.

BACKUP NODE (Back up a NAS node)

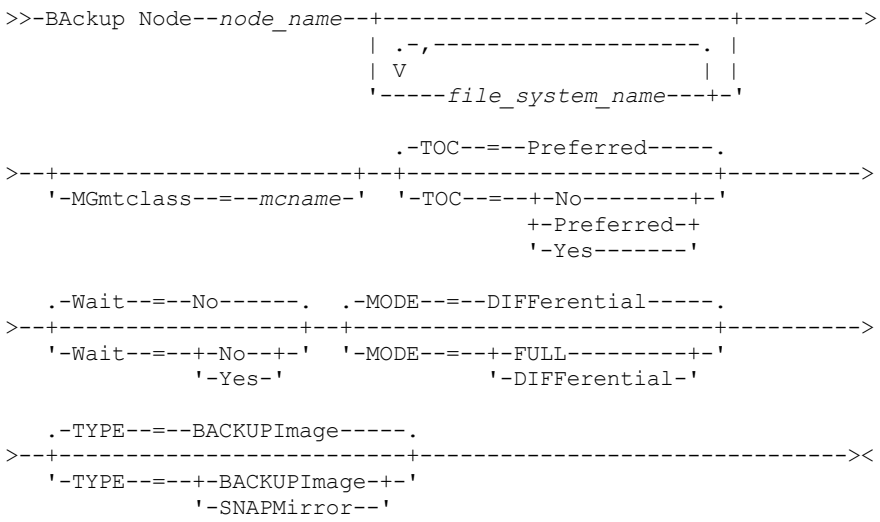
Use this command to start a backup operation for a network-attached storage (NAS) node.

Backups that are created for NAS nodes with this BACKUP NODE command are functionally equivalent to backups that are created by using the BACKUP NAS command on an IBM Spectrum Protect™ client. You can restore these backups with either the server's RESTORE NODE command or the client's RESTORE NAS command.

Privilege class

To issue this command, you must have system privilege, policy privilege for the domain to which the node is assigned, or client owner authority over the node.

Syntax



Parameters

node_name (Required)
Specifies the node for which the backup will be performed. You cannot use wildcard characters or specify a list of names.

file_system_name
Specifies the name of one or more file systems to back up. You can also specify names of virtual file spaces that have been defined for the NAS node. The file system name that you specify cannot contain wildcard characters. You can specify more than one file system by separating the names with commas and no intervening spaces.

If you do not specify a file system, all file systems will be backed up. Any virtual file spaces defined for the NAS node are backed up as part of the file system image, not separately.

If a file system exists on the NAS device with the same name as the virtual file space specified, IBM Spectrum Protect automatically renames the existing virtual file space in the server database, and backs up the NAS file system which matches the name specified. If the virtual file space has backup data, the file space definition associated with the virtual file space will also be renamed.

Tip: See the virtual file space name parameter in the DEFINE VIRTUALFSMAPPING command for more naming considerations.

In determining the file systems to process, the server will not use any DOMAIN.NAS, INCLUDE.FS.NAS, or EXCLUDE.FS.NAS statements in any client option file or client option set. If you back up multiple file systems, the backup of each file system is a separate server process.

MGmtclass
Specifies the name of the management class to which this backup data is bound. If you do not specify a management class, the backup data is bound to the default management class of the policy domain to which the node is assigned. In determining the management class, the server will *not* use any INCLUDE.FS.NAS statements in any client option file or client option set. The destination management class might refer to an IBM Spectrum Protect native pool, in which case Network Data Management Protocol (NDMP) data is sent into the IBM Spectrum Protect native hierarchy. After this occurs, the data stays in the IBM Spectrum Protect hierarchy. Data flowing to IBM Spectrum Protect native pools goes over the LAN and data flowing to NAS pools can be directly attached or over a SAN.

When you specify a management class with the BACKUP NODE command, all versions of the backup data that belong to the NAS node are rebound to the new management class.

TOC
Specifies whether a table of contents (TOC) is saved for each file system backup. Consider the following in determining whether you want to save a table of contents:

- If a table of contents is saved, you will be able to use the QUERY TOC command to determine the contents of a file system backup in conjunction with the RESTORE NODE command to restore individual files or directory trees. You can also use the IBM Spectrum Protect web backup-archive client to examine the entire file system tree and choose files and directories to restore. Creation of a table of contents requires that you define the TOCDESTINATION attribute in the backup copy group for the management class to which this backup image is bound. Creating a table of contents requires additional processing, network resources, storage pool space, and possibly a mount point during the backup operation.
- A table of contents for a NAS file system cannot have a directory path greater than 1024 characters.
- If a table of contents is not saved for a file system backup, you will still be able to restore individual files or directory trees using the RESTORE NODE command, provided that you know the fully qualified name of each file or directory to be restored and the image in which that object was backed up.

  This parameter is optional. The default value is Preferred. Possible values are:

  No
  Specifies that table of contents information is not saved for file system backups.
  Preferred
  Specifies that table of contents information should be saved for file system backups. However, a backup does not fail just because an error occurs during creation of the table of contents. This is the default value.
  Yes
  Specifies that table of contents information must be saved for each file system backup. A backup fails if an error occurs during creation of the table of contents.

Attention: If MODE=DIFFERENTIAL is specified and a table of contents is requested (TOC=PREFERRED or TOC=YES), but the last full image does not have a table of contents, a full backup will be performed and a table of contents will be created for that full backup.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. The default is NO. Possible values are:

No
: Specifies that the server processes this command in the background. Use the QUERY PROCESS command to monitor the background processing of this command.

Yes
: Specifies that the server processes this command in the foreground. You wait for the command to complete before continuing with other tasks. The server then displays the output messages to the administrative client when the command completes. If you are backing up multiple file systems, all backup processes must complete before the command is complete.
Attention: You cannot specify WAIT=YES from the server console.

MODE

Specifies whether the file system backups are full or differential. The default is DIFFERENTIAL.

FULL
: Specifies to back up the entire file system.

DIFFerential
: Specifies that only the files that have changed since the most recent full backup should be backed up. If you choose a differential backup, and a full backup is not found, a full backup is performed. You cannot specify TYPE=SNAPMIRROR when the MODE parameter is set to DIFFERENTIAL.

TYPE

Specifies the backup method used to perform the NDMP backup operation. The default value for this parameter is BACKUPIMAGE and it should be used to perform a standard NDMP base or differential backup. Other image types represent backup methods that might be specific to a particular file server. Possible values are:

BACKUPImage
: Specifies that the file system should be backed up using an NDMP dump operation. This is the default method for performing an NDMP backup. The BACKUPIMAGE type operation supports full and differential backups, file-level restore processing and directory-level backup.

SNAPMirror
: Specifies that the file system should be copied to an IBM Spectrum Protect storage pool using the NetApp SnapMirror to Tape function. SnapMirror images are block level full backup images of a file system. Typically, a SnapMirror backup takes significantly less time to perform than a traditional NDMP full file system backup. However there are limitations and restrictions on how SnapMirror images can be used. The SnapMirror to Tape function is intended to be used as a disaster-recovery option for copying very large NetApp file systems to secondary storage.

  For most NetApp file systems, use the standard NDMP full or differential backup method. Refer to the documentation that came with your NetApp file server for more information.

  When setting the TYPE parameter to SNAPMirror, the following restrictions apply:

  Restrictions:

  - You cannot specify TOC=YES or TOC=PREFERRED.
  - The file_system_name cannot be a virtual filespace name.
  - The snapshot which is created automatically by the file server during the SnapMirror copy operation will be deleted at end of the operation.
  - This parameter is valid for NetApp and IBM® N-Series file servers only.

Example: Perform a full backup

Perform a full backup on the /vol/vol10 file system of NAS node NAS1.

```
backup node nas1 /vol/vol10 mode=full
```

Example: Perform a backup on a directory and create a table of contents

Back up the directory /vol/vol2/mikes on the node NAS1 and create a table of contents for the image. For the following two examples, assume Table 1 contains the virtual file space definitions exist on the server for the node NAS1.

```
backup node nas1 /mikesdir
```

Table 1. Virtual file space definitions

Virtual file space name	File system	Path
/mikesdir	/vol/vol2	/mikes
/DataDirVol2	/vol/vol2	/project1/data
/TestDirVol1	/vol/vol1	/project1/test

Example: Perform a backup on two directories

Back up the directories /vol/vol2/project1/data and /vol/vol1/project1/test of the node NAS1. Refer to Table 1 for the virtual file space definitions that exist on the server for the node NAS1.

```
backup node nas1 /DataDirVol2,/testdirvol1  mode=full toc=yes
```

Related commands

Table 2. Commands related to BACKUP NODE

Command	Description
BACKUP NAS (client command)	Creates a backup of NAS node data.
CANCEL PROCESS	Cancels a background server process.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
QUERY NASBACKUP	Displays information about NAS backup images.
QUERY TOC	Displays details about the table of contents for a specified backup image.
QUERY COPYGROUP	Displays the attributes of a copy group.
RESTORE NAS (client command)	Restores a backup of NAS node data.
RESTORE NODE	Restores a network-attached storage (NAS) node.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

Related concepts:
Backup and restore using NetApp SnapMirror to Tape feature

BACKUP STGPOOL (Back up primary storage pool data to a copy storage pool)

Use this command to back up primary storage pool files to a copy storage pool.

You can back up data from a primary storage pool that is defined with the NATIVE, NONBLOCK, or any of the NDMP formats (NETAPPDUMP, CELERRADUMP, or NDMPDUMP). The copy storage pool to which data is to be backed up must have the same data format as the primary storage pool. IBM Spectrum Protect™ supports back-end data movement for NDMP images.

If a file exists in the copy storage pool, the file is not backed up unless the copy of the file in the copy storage pool is marked as damaged. However, a new copy is not created if the file in the primary storage pool is also marked as damaged. In a random-access storage pool, cached copies of migrated files and damaged primary files are not backed up.

Tip: Issuing this command for a primary storage pool that is set up for data deduplication removes duplicate data, if the copy storage pool is also set up for data deduplication.

If migration for a storage pool starts during a storage pool backup, some files might be migrated before they are backed up. You might want to back up storage pools that are higher in the migration hierarchy before you back up storage pools that are lower.

Restrictions:

- Do not run the MOVE DRMEDIA and BACKUP STGPOOL commands concurrently. Ensure that the storage pool backup processes are complete before you issue the MOVE DRMEDIA command.
- You cannot back up data from or to storage pools defined with a CENTERA device class.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the copy storage pool in which backup copies are to be produced.

Syntax

```
>>-BAckup STGpool--primary_pool_name--copy_pool_name------------>

   .-MAXPRocess--=--1------.
>--+----------------------+----------------------------------->
   '-MAXPRocess--=--number-'

   .-Preview--=--No-------------------.
>--+--------------------------------+-------------------------->
   '-Preview--=--+-No---------------+-'
                 +-Yes-------------+
                 |             (1) |
                 '-VOLumesonly-----'

   .-SHREDTONOshred--=--No------.  .-Wait--=--No------.
>--+---------------------------+--+------------------+-------><
   '-SHREDTONOshred--=--+-No--+-'  '-Wait--=--+-No--+-'
                        '-Yes-'               '-Yes-'
```

Notes:

1. Valid only for storage pools that are associated with a sequential-access device class.

Parameters

primary_pool (Required)
: Specifies the primary storage pool.

copy_pool (Required)
: Specifies the copy storage pool.

MAXPRocess
: Specifies the maximum number of parallel processes to use for backing up files. This parameter is optional. Enter a value 1 - 999. The default is 1.

  Using multiple, parallel processes can improve throughput for the backup. The expectation is that the time needed to complete the storage pool backup is decreased by using multiple processes. However, when multiple processes are running, in some cases one or more of the processes needs to wait to use a volume that is already in use by a different backup process.

  When you determine this value, consider the number of logical and physical drives that can be dedicated to this operation. To access a sequential access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect and system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the backup.

  Each process needs a mount point for copy storage pool volumes, and, if the device type is not FILE, each process also needs a drive. If you are backing up a sequential storage pool, each process needs an extra mount point for primary storage pool volumes and, if the device type is not FILE, an extra drive. For example, suppose that you specify a maximum of three processes to back up a primary sequential storage pool to a copy storage pool of the same device class. Each process requires two mount points and two drives. To run all three processes, the device class must have a mount limit of at least 6, and at least six mount points and six drives must be available.

  To preview a backup, only one process is used and no mount points or drives are needed.

Preview

Specifies whether you want to preview but not run the backup. The preview displays the number of files and bytes to be backed up and a list of the primary storage pool volumes that you must mount. This parameter is optional. The default is NO. You can specify the following values:

No
: Specifies that the backup is done.

Yes
: Specifies that you want to preview the backup but not do the backup.

VOLumesonly
: Specifies that you want to preview the backup only as a list of the volumes that must be mounted. This choice requires the least processing time. The VOLUMESONLY option is valid only for storage pools that are associated with a sequential-access device class.
The VOLUMESONLY option can be used to obtain a list of volumes that are needed by the storage pool backup process. For example:

```
backup stgpool primary_pool copystg preview=volumesonly
```

The list of volumes are logged in the server activity log with the ANR1228I message. Query the server activity log to get the list of volumes required. For example:

```
query actlog msg=1228
```

SHREDTONOshred
: Specifies whether data is backed up to a copy storage pool from a primary storage pool that enforces shredding. This parameter is optional. The default value is NO. You can specify the following values:

No
: Specifies that the server does not allow data to be backed up to a copy storage pool from a primary storage pool that enforces shredding. If the primary storage pool enforces shredding, the operation fails.

Yes
: Specifies that the server does allow data to be backed up to a copy storage pool from a primary storage pool that enforces shredding. The data in the copy storage pool is not shredded when it is deleted.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. You can specify the following values:

No
: Specifies that the server processes this command in the background.

You can continue with other tasks while the command is being processed. Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files might already have been backed up before the cancellation.

Yes
: Specifies that the server processes this operation in the foreground. You must wait for the operation to complete before you continue with other tasks. The server displays the output messages to the administrative client when the operation completes.
Note: You cannot specify WAIT=YES from the server console.

Example: Back up the primary storage pool

Back up the primary storage pool that is named PRIMARY_POOL to the copy storage pool named COPYSTG.

```
backup stgpool primary_pool copystg
```

Related commands

Table 1. Commands related to BACKUP STGPOOL

Command	Description
CANCEL PROCESS	Cancels a background server process.

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY PROCESS	Displays information about background processes.
QUERY SHREDSTATUS	Displays information about data waiting to be shredded.
QUERY STGPOOL	Displays information about storage pools.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
SHRED DATA	Manually starts the process of shredding deleted data.

BACKUP VOLHISTORY (Save sequential volume history information)

Use this command to back up sequential volume history information to one or more files.

Tip: You must use volume history information when you reload the database and audit affected storage pool volumes. If you cannot start the server, you can use the volume history file to query the database about these volumes.
The volume history includes information about the following types of volumes:

- Archive log volumes
- Database backup volumes
- Export volumes
- Backup set volumes
- Database snapshot volumes
- Database recovery plan file volumes
- Recovery plan file volumes
- Recovery plan file snapshot volumes
- The following sequential access storage pool volumes:
  - Volumes added to storage pools
  - Volumes reused through reclamation or MOVE DATA operations
  - Volumes removed by using the DELETE VOLUME command or during reclamation of scratch volumes

Attention: To restore a database, the server must use information from the volume history file and the device configuration file. You must make and save copies of the volume history file and the device configuration file. These files cannot be recreated.

AIX Linux You must use the VOLUMEHISTORY server option to specify one or more volume history files. IBM Spectrum Protect™ updates volume history files whenever server sequential volume history information is changed.

Windows At installation, the server options file includes a VOLUMEHISTORY option that specifies a default volume history file named volhist.out. IBM Spectrum Protect updates volume history files whenever server sequential volume history information is changed.

To ensure that updates are complete before the server is halted, follow these steps:

- Do not halt the server for a few minutes after you issue the BACKUP VOLHISTORY command.
- Specify multiple VOLUMEHISTORY options in the server options file.
- Examine the volume history file to see if the file has been updated.

Privilege class

Any administrator can issue this command unless it includes the FILENAMES parameter. If the FILENAMES parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES, the administrator must have system privilege. If the FILENAMES parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have operator, policy, storage or system privilege.

Syntax

```
>>-BAckup VOLHistory--+---------------------------------+------><
                     |               .-,-------------. |
                     |               V               | |
                     '-Filenames--=------file_name---+-'
```

Parameters

Filenames

Specifies the names of one or more files in which to store a backup copy of volume history information. Separate multiple file names with commas and no intervening spaces. This parameter is optional.

If you do not specify a file name, IBM Spectrum Protect stores the information in all files specified with the VOLUMEHISTORY option in the server options file.

Example: Back up the volume history information to a file

Back up the volume history information to a file called VOLHIST.

```
backup volhistory filenames=volhist
```

Related commands

Table 1. Commands related to BACKUP VOLHISTORY

Command	Description
DELETE VOLHISTORY	Removes sequential volume history information from the volume history file.
DELETE VOLUME	Deletes a volume from a storage pool.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
UPDATE VOLHISTORY	Adds or changes location information for a volume in the volume history file.

BEGIN EVENTLOGGING (Begin logging events)

Use this command to begin logging events to one or more receivers. A receiver for which event logging has begun is an *active receiver*.

When the server is started, event logging automatically begins for the console and activity log and for any receivers that are started automatically based on entries in the server options file. You can use this command to begin logging events to receivers for which event logging is *not* automatically started at server startup. You can also use this command after you have disabled event logging to one or more receivers.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                      .-ALL--------------------.
>>-BEGin EVentlogging--+-----------------------+-------------><
                       | .-,------------------. |
                       | V                    | |
                       '---+-CONSOLE---------+-+-'
                           +-ACTLOG----------+
                           +-EVENTSERVER-----+
                           +-FILE------------+
                           +-FILETEXT--------+
                           |             (1) |
                           +-NTEVENTLOG------+
```

```
|         (2)      |
+-SYSLOG----------+
+-TIVOLI----------+
'-USEREXIT-------'
```

Notes:

1. This parameter is only available for the Windows operating system.
2. This parameter is only available for the Linux operating system.

Parameters

Specify one or more receivers. You can specify multiple receivers by separating them with commas and no intervening spaces. If you specify ALL, logging begins for all receivers that are configured. The default is ALL.

ALL
: Specifies all receivers that are configured for event logging.

CONSOLE
: Specifies the server console as a receiver.

ACTLOG
: Specifies the IBM Spectrum Protect™ activity log as a receiver.

EVENTSERVER
: Specifies the event server as a receiver.

FILE
: Specifies a user file as a receiver. Each logged event is a record in the file and a person cannot read each logged event easily.

FILETEXT
: Specifies a user file as a receiver. Each logged event is a fixed-size, readable line.

Windows NTEVENTLOG
: Windows Specifies the Windows application log as a receiver.

Linux SYSLOG
: Linux Specifies the Linux system log as a receiver.

TIVOLI
: Specifies the Tivoli Management Environment (TME) as a receiver.

USEREXIT
: Specifies a user-written routine to which IBM Spectrum Protect writes information as a receiver.

Example: Begin logging events

Begin logging events to the IBM Spectrum Protect activity log.

```
begin eventlogging actlog
```

Related commands

Table 1. Commands related to BEGIN EVENTLOGGING

Command	Description
DISABLE EVENTS	Disables specific events for receivers.
ENABLE EVENTS	Enables specific events for receivers.
END EVENTLOGGING	Ends event logging to a specified receiver.
QUERY ENABLED	Displays enabled or disabled events for a specific receiver.
QUERY EVENTRULES	Displays information about rules for server and client events.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

CANCEL commands

Use the CANCEL commands to end a task or process before it is completed.

- CANCEL EXPIRATION (Cancel an expiration process)
- CANCEL EXPORT (Delete a suspended export operation)
- CANCEL PROCESS (Cancel an administrative process)
- CANCEL REPLICATION (Cancel node replication processes)
- CANCEL REQUEST (Cancel one or more mount requests)
- CANCEL RESTORE (Cancel a restartable restore session)
- CANCEL SESSION (Cancel one or more client sessions)

CANCEL EXPIRATION (Cancel an expiration process)

Use this command to cancel a process with an unknown process number that is running as a result of an inventory expiration operation.

Use the CANCEL EXPIRATION command if the expiration process number is not known, otherwise use the CANCEL PROCESS and specify the process number of the expiration process. Both commands call the same code to end the expiration process.

You can use the CANCEL EXPIRATION command to automate the cancellation of an expiration process. For example, if you start inventory expiration at midnight and, due to the maintenance workload on the server, the process must finish at 03:00, you can schedule a CANCEL EXPIRATION command to run at 03:00 without knowing the process number.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-CANcel EXPIration-----------------------------------------><
```

Example: Cancel an inventory expiration process

Cancel the process that was generated by an inventory expiration operation.

```
cancel expiration
```

Related commands

Table 1. Command related to CANCEL EXPIRATION

Command	Description
QUERY PROCESS	Displays information about background processes.
EXPIRE INVENTORY	Manually starts inventory expiration processing.

CANCEL EXPORT (Delete a suspended export operation)

Use this command to delete a suspended server-to server export operation. After issuing the CANCEL EXPORT command, you cannot restart the export operation. Issue the CANCEL PROCESS command to delete a currently running export operation.

Privilege class

You must have system privilege to issue this command.

Syntax

```
                .-*--------------------.
>>-CANcel EXPort -+----------------------+--------------------><
                 '---export_identifier---'
```

Parameters

export_identifier
: The unique identifier of the suspended export operation that you wish to delete. You can also enter wildcard characters for the identifier. Issue the QUERY EXPORT command to list the currently suspended export operations.

Example: Delete a specific suspended export operation

Cancel the suspended server-to-server export operation EXPORTALLACCTNODES.

```
cancel export exportallacctnodes
```

Example: Delete all suspended server-to-server export operations

Cancel all suspended server-to-server export processes.

```
cancel export *
```

Related commands

Table 1. Commands related to CANCEL EXPORT

Command	Description
CANCEL PROCESS	Cancels a background server process.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

CANCEL PROCESS (Cancel an administrative process)

Use this command to cancel a background process started by an administrative command or by a process, such as storage pool migration.

The following commands generate background processes:

- AUDIT CONTAINER
- AUDIT LIBRARY
- AUDIT LICENSES
- AUDIT VOLUME
- BACKUP DB
- BACKUP NODE
- BACKUP STGPOOL
- CHECKIN LIBVOLUME
- CHECKOUT LIBVOLUME
- AIX Linux Windows CONVERT STGPOOL
- DELETE FILESPACE
- DELETE VOLUME
- EXPIRE INVENTORY
- EXPORT ADMIN
- EXPORT NODE
- EXPORT POLICY
- EXPORT SERVER
- GENERATE BACKUPSET
- IMPORT ADMIN

- IMPORT NODE
- IMPORT POLICY
- IMPORT SERVER
- MIGRATE STGPOOL
- MOVE DATA
- MOVE DRMEDIA
- MOVE MEDIA
- PREPARE
- PROTECT STGPOOL
- RECLAIM STGPOOL
- REPLICATE NODE
- RESTORE NODE
- RESTORE STGPOOL
- RESTORE VOLUME
- VARY

The following internal server operations generate background processes:

- Inventory expiration
- Migration
- Reclamation

To cancel a process, you must have the process number, which you can obtain by issuing the QUERY PROCESS command.

Some processes, such as reclamation, generate mount requests to complete processing. If a process has a pending mount request, the process might not respond to a CANCEL PROCESS command until the mount request is answered or canceled by using the REPLY or CANCEL REQUEST command, or by timing out.

Issue the QUERY REQUEST command to list open requests, or query the activity log to determine whether a process has a pending mount request. A mount request indicates that a volume is needed for the current process, but the volume is not available in the library. The volume might not be available if the administrator issues the MOVE MEDIA or CHECKOUT LIBVOLUME command, or manually removes the volume from the library.

After you issue a CANCEL PROCESS command for an export operation, the process cannot be restarted. To stop a server-to-server export operation but allow it to be restarted later, issue the SUSPEND EXPORT command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-CANcel PRocess--process_number-----------------------------><
```

Parameters

process_number (Required)
Specifies the number of the background process you want to cancel.

Example: Cancel a background process by using its process number

Cancel background process number 3.

```
cancel process 3
```

Related commands

Table 1. Commands related to CANCEL PROCESS

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.

Command	Description
CANCEL REQUEST	Cancels pending volume mount requests.
AIX Linux Windows CONVERT STGPOOL	AIX Linux Windows Convert a storage pool to a directory-container storage pool.
AIX Linux Windows PROTECT STGPOOL	AIX Linux Windows Protects a directory-container storage pool.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
QUERY PROCESS	Displays information about background processes.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
REPLY	Allows a request to continue processing.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

CANCEL REPLICATION (Cancel node replication processes)

Use this command to cancel all node replication processes.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-CANcel REPLication-----------------------------------------><
```

Parameters

None.

Example: Cancel node replication processes

Cancel all node replication processes.

```
cancel replication
```

Related commands

Table 1. Commands related to CANCEL REPLICATION

Command	Description
QUERY PROCESS	Displays information about background processes.
QUERY REPLICATION	Displays information about node replication processes.

CANCEL REQUEST (Cancel one or more mount requests)

Use this command to cancel one or more pending media mount requests. To cancel a mount request, you need to know the request number assigned to the request. This number is included in the mount request message and can also be shown by using the QUERY REQUEST command.

Privilege class

To issue this command, you must have system privilege or operator privilege.

Syntax

```
>>-CANcel REQuest--+-request_number-+--+-----------+-----------><
                   '-ALl------------'  '-PERManent-'
```

Parameters

request_number
: Specifies the request number of the mount request to cancel.

ALl
: Specifies to cancel all pending mount requests.

PERManent
: Specifies that you want the server to flag the volumes for which you are canceling a mount request as unavailable. This parameter is optional.

Example: Cancel a mount request

Cancel request number 2.

```
cancel request 2
```

Related commands

Table 1. Commands related to CANCEL REQUEST

Command	Description
QUERY REQUEST	Displays information about all pending mount requests.
UPDATE VOLUME	Updates the attributes of storage pool volumes.

CANCEL RESTORE (Cancel a restartable restore session)

Use this command to cancel a restartable restore session. You can cancel restore sessions in the active or restartable state. Any outstanding mount requests related to this session are automatically canceled.

To display restartable restore sessions, use the QUERY RESTORE command.

Privilege class

To issue this command, you must have system or operator privilege.

Syntax

```
>>-CANcel--RESTore--+-session_number-+-------------------------><
                    '-ALl------------'
```

Parameters

session_number
: Specifies the number for the restartable restore session. An active session is a positive number, and a restartable session is a negative number.

ALl
: Specifies that all the restartable restore sessions are to be canceled.

Example: Cancel restore operations

Cancel all restore operations.

```
cancel restore all
```

Related commands

Table 1. Commands related to CANCEL RESTORE

Command	Description
QUERY RESTORE	Displays information about restartable restore sessions.

CANCEL SESSION (Cancel one or more client sessions)

Use this command to cancel existing administrative or client node sessions, and to force an administrative or client node session off the server. Any outstanding mount requests related to this session are automatically canceled. The client node must start a new session to resume activities.

If you cancel a session that is in the idle wait (IdleW) state, the client session is automatically reconnected to the server when it starts to send data again.

If this command interrupts a process, such as backup or archive, the results of any processing active at the time of interruption are rolled back and not committed to the database.

Privilege class

To issue this command, you must have system or operator privilege.

Syntax

```
>>-CANcel SEssion--+-session_number-+-------------------------><
                   '-ALl------------'
```

Parameters

session_number
: Specifies the number of the administrative, server, or client node sessions that you want to cancel.

ALl
: Specifies that all client node sessions are canceled. You cannot use this parameter to cancel administrative client or server sessions.

Example: Cancel a specific client node session

Cancel the client node session with NODEP (session 3).

```
cancel session 3
```

Related commands

Table 1. Commands related to CANCEL SESSION

Command	Description
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
LOCK ADMIN	Prevents an administrator from accessing IBM Spectrum Protect.
LOCK NODE	Prevents a client from accessing the server.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.

CHECKIN LIBVOLUME (Check a storage volume into a library)

Use this command to add a sequential access storage volume or a cleaning tape to the server inventory for an automated library. The server cannot use a volume that physically resides in an automated library until that volume is checked in.

Important:

1. The CHECKIN LIBVOLUME command processing does not wait for a drive to become available, even if the drive is only in the IDLE state. If necessary, you can make a library drive available issuing the DISMOUNT VOLUME command to dismount the volume. After a library drive is available, reissue the CHECKIN LIBVOLUME command.
2. You do not define the drives, check in media, or label the volumes in an external library. The server provides an interface that external media management systems use to operate with the server.
3. When you check in WORM tapes other than 3592, you must use CHECKLABEL=YES or they are checked in as normal read/write tapes.

This command creates a background process that you can cancel with the CANCEL PROCESS command. To display information about background processes, use the QUERY PROCESS command.

For detailed and current drive and library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax for SCSI libraries

```
>>-CHECKIn LIBVolume--library_name------------------------------>

                    .-SEARCH--=--No-.
>----+-volume_name--+---------------+-+------------------------>
     +-SEARCH--=--Yes--+-------+------+
     |                 '-| A |-'      |
     '-SEARCH--=--Bulk--+-------+-----'
                        '-| A |-'

                           .-OWNer--=--""----------.
>--STATus--=--+-PRIvate-+--+-----------------------+------------>
              +-SCRatch-+  '-OWNer--=--server_name-'
              '-CLEaner-'

   .-CHECKLabel--=--Yes---------.  .-SWAP--=--No------.
>--+----------------------------+--+------------------+--------->
   '-CHECKLabel--=--+-Yes-----+-'  '-SWAP--=--+-No--+-'
                    +-No------+               '-Yes-'
                    '-Barcode-'

   .-WAITTime--=--60----.
>--+--------------------+--+-------------------------+-------><
   '-WAITTime--=--value-'  '-CLEanings--=----number---'

A (SEARCH=Yes, SEARCH=Bulk)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.              |
   |               V             |              |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Syntax for 349X libraries

```
>>-CHECKIn LIBVolume--library_name------------------------------>
```

```
                    .-SEARCH--=--No-.
>----+-volume_name--+---------------+-+------------------------>
     '-SEARCH--=--Yes--+-------+------'
                       '-| A |-'

                            .-OWNer--=--""----------.
>--STATus--=--+-PRIvate-+--+----------------------+------------>
              '-SCRatch-'  '-OWNer--=--server_name-'

   .-CHECKLabel--=--Yes-----.
>--+------------------------+--+---------------------+--------->
   '-CHECKLabel--=--+-Yes-+-'  '-DEVType--=--+-3590-+-'
                    '-No--'                  '-3592-'

   .-SWAP--=--No------.  .-WAITTime--=--60----.
>--+------------------+--+--------------------+---------------><
   '-SWAP--=--+-No--+-'  '-WAITTime--=--value-'
              '-Yes-'

A (SEARCH=Yes)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.              |
   |               V             |              |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Syntax for ACSLS libraries

```
>>-CHECKIn LIBVolume--library_name------------------------------>

                    .-SEARCH--=--No-.
>----+-volume_name--+---------------+-+------------------------>
     '-SEARCH--=--Yes--+-------+------'
                       '-| A |-'

                            .-OWNer--=--""----------.
>--STATus--=--+-PRIvate-+--+----------------------+------------>
              '-SCRatch-'  '-OWNer--=--server_name-'

   .-CHECKLabel--=--Yes-----.  .-SWAP--=--No------.
>--+------------------------+--+------------------+------------>
   '-CHECKLabel--=--+-Yes-+-'  '-SWAP--=--+-No--+-'
                    '-No--'               '-Yes-'

   .-WAITTime--=--60----.
>--+--------------------+-------------------------------------><
   '-WAITTime--=--value-'

A (SEARCH=Yes)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.              |
   |               V             |              |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Parameters

library_name (Required)
: Specifies the name of the library.

volume_name
: Specifies the volume name of the storage volume that is being checked in. This parameter is required if SEARCH equals NO. Do not enter this parameter if the SEARCH parameter equals YES or BULK. If you are checking a volume into a SCSI library with multiple entry/exit ports, the volume in the lowest numbered slot is checked in.

STATus (Required)
: Specifies the volume status. Possible values are:

PRIvate
Specifies that the volume is a private volume that is mounted only when it is requested by name.

SCRatch
Specifies that the volume is a new scratch volume. This volume can be mounted to satisfy scratch mount requests during either data storage operations or export operations.

If a volume has an entry in volume history, you cannot check it in as a scratch volume.

CLEaner
Specifies that the volume is a cleaner cartridge and not a data cartridge. The CLEANINGS parameter is required for a cleaner cartridge and must be set to the number of cleaner uses.

CHECKLABEL=YES is not valid for checking in a cleaner cartridge. Use STATUS=CLEANER to check in a cleaner cartridge separately from a data cartridge.

OWNer
Specifies which library client owns a private volume in a library that is shared across a SAN. The volume for which you specify ownership must be a private volume. You cannot specify ownership for a scratch volume. Furthermore, you cannot specify an owner when you use SEARCH=YES or SEARCH=BULK.

When you issue the CHECKIN LIBVOLUME command, the server validates the owner. If you did not specify this parameter, then the server uses the default and delegates volume ownership to the owning library client, as recorded in the volume history file on the library manager. If the volume is not owned by any library client, then the server delegates ownership to the library manager.

SEARCH
Specifies whether the server searches the library to find volumes that were not checked in. This parameter is optional. The default is NO.

Possible values are:

No
Specifies that only the named volume is checked into the library.

For SCSI libraries: The server issues a request to have the volume inserted into a cartridge slot in the library or, if available, into an entry port. The cartridge slot or entry port is identified by its element address. **For 349X libraries:** The volume might already be in the library, or you can put it into the I/O station when prompted.

Yes
Specifies that the server searches the library for volumes to be checked in. You can use the VOLRANGE or VOLLIST parameter to limit the search. When you use this parameter, consider the following restrictions:

- If the library is shared between applications, the server might examine a volume that is required by another application. For 349X libraries, the server queries the library manager to determine all volumes that are assigned to the SCRATCH or PRIVATE category and to the INSERT category.
- For SCSI libraries, do not specify both SEARCH=YES and CHECKLABEL=NO in the same command.

Bulk
Specifies that the server searches the library's entry/exit ports for volumes that can be checked in automatically. This option applies to only SCSI libraries.
Important:

1. Do not specify both CHECKLABEL=NO and SEARCH=BULK.
2. You can use the VOLRANGE or VOLLIST parameter to limit the search.

VOLRange
Specifies a range of volume names that are separated by commas. You can use this parameter to limit the search for volumes to be checked in when you specify SEARCH=YES (349X, ACSLS, and SCSI libraries) or SEARCH=BULK (SCSI libraries only). If there are no volumes in the library that are within the specified range, the command completes without errors.

Specify only volume names that can be numerically incremented. In addition to the incremental area, a volume name can include an alphanumeric prefix and an alphanumeric suffix, for example:

Parameter	Description

Parameter	Description
`volrange=bar110,bar130`	The 21 volumes are checked in: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	The 3 volumes are checked in: bar11a, bar12a, bar13a.
`volrange=123400,123410`	The 11 volumes are checked in: 123400, 123401, ...123409, 123410.

VOLList

Specifies a list of volumes. You can use this parameter to limit the search for volumes to be checked in when you specify SEARCH=YES (349X, ACSLS, and SCSI libraries) or SEARCH=BULK (SCSI libraries only). If there are no volumes in the library that are in the list, the command completes without errors.
Possible values are:

volume_name

Specifies one or more volumes names that are separated by commas and no intervening spaces. For example: VOLLIST=TAPE01,TAPE02.

FILE: file_name

Specifies the name of a file that contains a list of volumes for the command. In the file, each volume name must be on a separate line. Blank lines and comment lines that begin with an asterisk are ignored. For example, to use volumes TAPE01, TAPE02 and TAPE03, create a file, TAPEVOL, that contains these lines:

```
TAPE01
TAPE02
TAPE03
```

You can specify the volumes for the command as follows: VOLLIST=FILE:TAPEVOL.

Attention: The file name is case-sensitive.

CHECKLabel

Specifies how or whether the server should read sequential media labels of volumes. This parameter is optional. The default is YES.
Possible values are:

Yes

Specifies that an attempt is made to read the media label during check-in.
Attention:

1. For SCSI libraries, do not specify both SEARCH=YES and CHECKLABEL=NO in the same command.
2. For WORM media other than 3592, you must specify YES.

No

Specifies that the media label is not read during check-in. However, suppressing label checking can result in future errors (for example, either a wrong label or an improperly labeled volume can cause an error). For 349X and ACSLS libraries, specify NO to avoid loading cartridges into a drive to read the media label. These libraries always return the external label information about cartridges, and IBM Spectrum Protect™ uses that information.

Barcode

Specifies that the server reads the bar code label if the library has a bar code reader and the volumes have external bar code labels. You can decrease the check-in time by using the bar code. This parameter applies only to SCSI libraries.

If the bar code reader cannot read the bar code label, or if the tape does not have a bar code label, the server mounts the tape and reads the internal label.

DEVType

Specifies the device type for the volume that is being checked in. This parameter is required if none of the drives in this library have defined paths.

3590

Specifies that the device type for the volume that is being checked in is 3590.

3592

Specifies that the device type for the volume that is being checked in is 3592.

SWAP
: Specifies whether the server swaps volumes if an empty library slot is not available. The volume that is selected for the swap operation (target swap volume) is ejected from the library and replaced with the volume that is being checked in. The server identifies a target swap volume by checking for an available scratch volume. If none exists, the server identifies the least frequently mounted volume.

  This parameter is optional. The default is NO. This parameter applies only if there is a volume name that is specified in the command. Possible values are:

  No
  : Specifies that the server checks in the volume only if an empty slot is available.

  Yes
  : Specifies that if an empty slot is not available, the server swaps cartridges to check in the volume.

WAITTime
: Specifies the number of minutes that the server waits for you to reply or respond to a request. Specify a value in the range 0-9999. If you want to be prompted by the server, specify a wait time greater than zero. The default value is 60 minutes. For example, suppose the server prompts you to insert a tape into the entry/exit port of a library. If you specified a wait time of 60 minutes, the server issues a request and waits 60 minutes for you to reply. Suppose, on the other hand, you specify a wait time of 0. If you already inserted a tape, a wait time of zero causes the operation to continue without prompting. If you have *not* inserted a tape, a wait time of zero will cause the operation to fail.

CLEanings
: Enter the recommended value for the individual cleaner cartridge (usually indicated on the cartridge). Cleanings apply only to SCSI libraries. This parameter is required if STATUS=CLEANER.

  If more than one cleaner is checked into the library, only one is used until its CLEANINGS value decreases to zero. Another cleaner is then selected, and the first cleaner can be checked out and discarded.

Example: Check a volume into a SCSI library

Check in a volume named `WPDV00` into the SCSI library named AUTO.

```
checkin libvolume auto wpdv00 status=scratch
```

Example: Use a bar code reader to scan a library for a cleaner cartridge

Scan a SCSI library named `AUTOLIB1` and, using the bar code reader, look for cleaner cartridge `CLNV`. Use SEARCH=YES, but limit the search by using the VOLLIST parameter.

```
checkin libvolume autolib1 search=yes vollist=cleanv status=cleaner
  cleanings=10 checklabel=barcode
```

Example: Scan a library to put unused volumes in a specific range in scratch status

Scan a 349X library named ABC, and limit the search to a range of unused volumes `BAR110` to `BAR130` and put them in scratch status.

```
checkin libvolume abc search=yes volrange=bar110,bar130
 status=scratch
```

Example: Scan a library to put a specific volume in scratch status

Use the barcode reader to scan a SCSI library named `MYLIB` for `VOL1`, and put it in scratch status.

```
checkin libvolume mylib search=yes vollist=vol1 status=scratch
 checklabel=barcode
```

Related commands

Table 1. Commands related to CHECKIN LIBVOLUME

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.

Command	Description
CANCEL PROCESS	Cancels a background server process.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DISMOUNT VOLUME	Dismounts a sequential, removable volume by the volume name.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.
QUERY PROCESS	Displays information about background processes.
REPLY	Allows a request to continue processing.
UPDATE LIBVOLUME	Changes the status of a storage volume.

CHECKOUT LIBVOLUME (Check a storage volume out of a library)

Use this command to remove a sequential access storage volume from the server inventory for an automated library. This command creates a background process that can be canceled with the CANCEL PROCESS command. To display information on background processes, use the QUERY PROCESS command.

Restrictions:

1. Check out processing does not wait for a drive to become available, even if the drive is in the IDLE state. If necessary, you can make a library drive available by dismounting the volume with the DISMOUNT VOLUME command. After a drive is available, the CHECKOUT LIBVOLUME command can be reissued.
2. Before checking out volumes from a 349X library, ensure that the 349x Cartridge Input and Output facility has enough empty slots for the volumes to be checked out. The 3494 Library Manager does not inform an application that the Cartridge Input and Output facility is full. It accepts requests to eject a cartridge and waits until the Cartridge Input and Output facility is emptied before returning to the server. IBM Spectrum Protect™ might appear to be hung when it is not. Check the library and clear any intervention requests.
3. Before checking volumes out of an ACSLS library, ensure that the CAP priority in ACSLS is greater than zero. If the CAP priority is zero, then you must specify a value for the CAP parameter on the CHECKOUT LIBVOLUME command.

For detailed and current drive and library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax for SCSI library

```
>>-CHECKOut LIBVolume--library_name----+-volume_name-+---------->
                                       '-| A |-------'

   .-REMove--=--Bulk-----.  .-CHECKLabel--=--Yes-----.
>--+--------------------+--+-----------------------+---------->
   '-REMove--=--+-Yes--+-'  '-CHECKLabel--=--+-Yes-+-'
                +-No---+                     '-No--'
                '-Bulk-'

   .-FORCE--=--No------.
>--+-------------------+-------------------------------------><
   '-FORCE--=--+-No--+-'
               '-Yes-'

A

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.               |
   |               V             |               |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Syntax for 349X library

```
>>-CHECKOut LIBVolume--library_name----+-volume_name-+---------->
                                       '-| A |-------'

   .-REMove--=--Bulk-----.
>--+--------------------+------------------------------------><
   '-REMove--=--+-Yes--+-'
                +-No---+
                '-Bulk-'

A

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.               |
   |               V             |               |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Syntax for ACSLS library

```
>>-CHECKOut LIBVolume--library_name----+-volume_name-+---------->
                                       '-| A |-------'

   .-REMove--=--Yes------.
>--+--------------------+--+------------------+-------------><
   '-REMove--=--+-Yes--+-'  '-CAP--=----x,y,z---'
                +-No---+
                '-Bulk-'

A

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.               |
   |               V             |               |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Parameters

library_name (Required)
: Specifies the name of the library.

volume_name

Specifies the volume name.

VOLRange

Specifies two volume names separated by a comma. This parameter is a range of volumes to be checked out. If there are no volumes in the library that are within the specified range, the command completes without errors.

Specify only volume names that can be numerically incremented. In addition to the incremental area, a volume name can include an alphanumeric prefix and an alphanumeric suffix, for example:

Parameter	Description
`volrange=bar110,bar130`	The 21 volumes are checked out: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	The 3 volumes are checked out: bar11a, bar12a, bar13a.
`volrange=123400,123410`	The 11 volumes are checked out: 123400, 123401, ...123409, 123410.

VOLList

Specifies a list of volumes to check out. If there are no volumes in the library that are in the list, the command completes without errors.

Possible values are:

volume_name

Specifies the names of one or more values that are used for the command. Example: VOLLIST=TAPE01,TAPE02.

FILE:file_name

Specifies the name of a file that contains a list of volumes for the command. In the file, each volume name must be on a separate line. Blank lines and comment lines that begin with an asterisk are ignored. For example, to use volumes TAPE01, TAPE02 and TAPE03, create a file, TAPEVOL, that contains these lines:

```
TAPE01
TAPE02
TAPE03
```

You can specify the volumes for the command as follows: VOLLIST=FILE:TAPEVOL.

Attention: The file name is case-sensitive.

REMove

Specifies that the server tries to move the volume out of the library and into the convenience I/O station or entry/exit ports. This parameter is optional. Possible values, depending on the type of library, are YES, BULK, and NO. The response of the server to each of those options and the default values are described in the following sections.

349X libraries: The default is BULK. The following table shows how the server responds for 349X libraries.

Table 1. How the server responds for 349X libraries

REMOVE=YES	REMOVE=BULK	REMOVE=NO
The 3494 Library Manager ejects the cartridge to the convenience I/O station.	The 3494 Library Manager ejects the cartridge to the high-capacity output facility.	The 3494 Library Manager does not eject the volume. The server leaves the cartridge in the library in the INSERT category for use by other applications.

SCSI libraries: The default is BULK. The following table shows how the server responds for a SCSI libraries.

Table 2. How the server responds for SCSI libraries

If a library . . .	And REMOVE=YES, then...	And REMOVE=BULK, then...	And REMOVE=NO, then...

If a library . . .	And REMOVE=YES, then...	And REMOVE=BULK, then...	And REMOVE=NO, then...
Does not have entry/exit ports	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.
Has entry/exit ports and an entry/exit *port is available*	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.
Has entry/exit ports, but *no ports are available*	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server waits for an entry/exit port to be made available.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.

ACSLS libraries: The default is YES. If the parameter is set to YES, and the cartridge access port (CAP) has an automatic selection priority value of 0, you must specify a CAP ID. The following table shows how the server responds for ACSLS libraries.

Table 3. How the server responds for ACSLS libraries

REMOVE=YES or REMOVE=BULK	REMOVE=NO
The server ejects the cartridge to the convenience I/O station, and deletes the volume entry from the server library inventory.	The server does not eject the cartridge. The server deletes the volume entry from the server library inventory and leaves the volume in the library.

CHECKLabel

Specifies how or whether the server reads sequential media labels of volumes.
Attention: This parameter does not apply to IBM® 349X or ACSLS libraries.
This parameter is optional. The default is YES. Possible values are:

Yes

Specifies that the server attempts to read the media label to verify that the correct volume is being checked out.

No

Specifies that during checkout the media label is not read. This improves performance because the read process does not occur.

FORCE

Specifies whether the server checks out a volume if an input/output (I/O) error occurs when reading the label.
Attention: This parameter does not apply to IBM 349X or ACSLS libraries.
This parameter is optional. The default is NO. Possible values are:

No
The server does not check out a storage volume if an I/O error occurs when reading the label.

Yes
The server checks out the storage volume even if an I/O error occurs.

CAP
Specifies which cartridge access port (CAP) to use for ejecting volumes if you specify REMOVE=YES. This parameter applies to volumes in ACSLS libraries only. If the CAP priority value is set to 0 in the library, this parameter is required. If a CAP priority value greater than 0 is set in the library, this parameter is optional. By default, all CAPs initially have a priority value of 0, which means that ACSLS does not automatically select the CAP.
To display valid CAP identifiers (*x,y,z*), issue the QUERY CAP command with ALL specified from the Automated Cartridge System System Administrator (ACSSA) console on the ACSLS server host. The identifiers are as follows:

x
The Automated Cartridge System (ACS) ID. This identifier can be a number in the range 0 - 126.

y
The Library Storage Module (LSM) ID. This identifier can be a number in the range 0 - 23.

z
The CAP ID. This identifier can be a number in the range 0 - 11.

For more information, see the StorageTek documentation.

Example: Check out a volume and check the label

Check out the volume that is named EXB004 from the library named FOREST. Read the label to verify the volume name, but do not move the volume out of the library.

```
checkout libvolume forest exb004 checklabel=yes remove=no
```

Related commands

Table 4. Commands related to CHECKOUT LIBVOLUME

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CANCEL PROCESS	Cancels a background server process.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.
QUERY PROCESS	Displays information about background processes.
REPLY	Allows a request to continue processing.
UPDATE LIBVOLUME	Changes the status of a storage volume.

CLEAN DRIVE (Clean a drive)

Use this command when you want IBM Spectrum Protect™ to immediately load a cleaner cartridge into a drive regardless of the cleaning frequency.

There are special considerations if you plan to use this command with a SCSI library that provides automatic drive cleaning through its device hardware.

Restriction: You cannot run the CLEAN DRIVE command for a drive whose only path source is a NAS file server.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-CLEAN DRIVE--library_name--drive_name----------------------><
```

Parameters

library_name (Required)
: Specifies the name of the library to which the drive is assigned.

drive_name (Required)
: Specifies the name of the drive.

Example: Clean a specific tape drive

You have already defined a library named AUTOLIB by using the DEFINE LIBRARY command, and you have already checked a cleaner cartridge into the library using the CHECKIN LIBVOL command. Inform the server that TAPEDRIVE3 in this library requires cleaning.

```
clean drive autolib tapedrive3
```

Related commands

Table 1. Commands related to CLEAN DRIVE

Command	Description
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE DRIVE	Deletes a drive from a library.
QUERY DRIVE	Displays information about drives.
UPDATE DRIVE	Changes the attributes of a drive.

COMMIT (Control committing of commands in a macro)

Use this command to control when a command is committed in a macro and to update the database when commands complete processing. When issued from the console mode of the administrative client, this command does not generate a message.

If an error occurs while processing the commands in a macro, the server stops processing the macro and rolls back any changes (since the last COMMIT). After a command is committed, it cannot be rolled back.

Ensure that your administrative client session is not running with the ITEMCOMMIT option if you want to control command processing. The ITEMCOMMIT option commits commands inside a script or a macro as *each* command is processed.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-COMMIT-----------------------------------------------------><
```

Parameters

None.

Example: Control committing of commands in a macro

From the interactive mode of the administrative client, register and grant authority to new administrators using a macro named REG.ADM. Changes are committed after each administrator is registered and is granted authority.

Macro Contents:

```
/* REG.ADM-register policy admin & grant authority*/
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
COMMIT  /* Commits changes */
REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
COMMIT  /* Commits changes */
```

Command

```
macro reg.adm
```

Related commands

Table 1. Commands related to COMMIT

Command	Description
MACRO	Runs a specified macro file.
ROLLBACK	Discards any uncommitted changes to the database since the last COMMIT was executed.

Related concepts:
Administrative client macros

AIX | Linux | Windows

CONVERT STGPOOL (Convert a storage pool to a container storage pool)

Use this command to convert a primary storage pool that uses a FILE device class, a tape device class, or a virtual tape library (VTL) to a directory-container or a cloud-container storage pool. You can use container storage pools for both inline and client-side data deduplication.

Restrictions: The following restrictions apply to storage pool conversion:

- You can convert a storage pool only once.
- You cannot update the storage pool during conversion processing. Migration and data movement processes are unavailable.
- You must update all policies to ensure that the destination specifies a storage pool that is not converted or undergoing conversion.

During conversion processing, all data from the source storage pool is moved to the target storage pool. When the process is completed, the source storage pool becomes unavailable. When a storage pool is unavailable, you are unable to write any data to it. The source storage pool is eligible for deletion but is not automatically deleted. You can restore data from the source storage pool if necessary.
Attention: During storage pool conversion, data is deleted from copy storage pools and active-data storage pools. This action occurs even if you specified the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool.

Privilege class

To issue this command, you must have restricted storage privilege.

Syntax

```
>>-CONvert STGpool--source_stgpool--target_stgpool-------------->
```

```
   .-MAXPRocess--=--8----------.
>--+---------------------------+--+----------------------+-----><
   '-MAXPRocess--=----number---'  '-DUration--=--minutes-'
```

Parameters

source_stgpool (Required)
: Specify a primary storage pool that uses a FILE device class, a tape device class, or a virtual tape library (VTL) for backup and archive processing. This parameter is required.

target_stgpool (Required)
: Specify the name of an existing directory-container or cloud-container storage pool that the storage pool is converted to. This parameter is required the first time that you issue this command.
: Tip: If you restart storage pool conversion and the target storage pool is different than the value that is specified the first time that you issued the CONVERT STGPOOL command, the command fails.

MAXPRocess
: Specifies the maximum number of parallel processes that can be used to convert data in the storage pool. This parameter is optional. You can specify a number in the range 1 - 99. The default value is 8.
: Tip: Changes to the default value are automatically saved. If you restart storage pool conversion and the parameter value is different than the value that is specified the first time that you issued the CONVERT STGPOOL command, the most recently specified value is used.

DUration
: Specifies the maximum number of minutes that a conversion should take before it is canceled. When the specified number of minutes elapses, the server cancels all conversion processes for the storage pool. You can specify a number in the range 1 - 9999. This parameter is optional. If you do not specify this parameter, the conversion runs until it is completed.
: Tip: Storage pool conversion for large storage pools can take days to complete. Use this parameter to limit the amount of time for storage pool conversion daily. As a best practice, schedule conversion for at least 2 hours for a storage pool that uses a FILE type device class and at least 4 hours for VTL.

Example: Convert a storage pool and specify a maximum number of processes

Convert a storage pool that is named DEDUPPOOL1, move the data to a container storage pool that is named DIRPOOL1, and specify 25 maximum processes.

```
convert stgpool deduppool1 dirpool1 maxprocess=25
```

Table 1. Commands related to CONVERT STGPOOL

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY CLEANUP	Query the cleanup status of a source storage pool.
QUERY CONVERSION	Query conversion status of a storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
REMOVE DAMAGED	Removes damaged data from a source storage pool.

COPY commands

Use the COPY commands to create a copy of IBM Spectrum Protect™ objects or data.

- COPY ACTIVEDATA (Copy active backup data from a primary storage pool to an active-data pool)
- COPY CLOPTSET (Copy a client option set)
- COPY DOMAIN (Copy a policy domain)
- COPY MGMTCLASS (Copy a management class)
- COPY POLICYSET (Copy a policy set)
- COPY PROFILE (Copy a profile)
- COPY SCHEDULE (Copy a client or an administrative command schedule)
- COPY SCRIPT (Copy an IBM Spectrum Protect script)
- COPY SERVERGROUP (Copy a server group)

COPY ACTIVEDATA (Copy active backup data from a primary storage pool to an active-data pool)

Use this command to copy active versions of backup data from a primary storage pool to an active-data pool. The primary benefit of active-data pools is fast client restores. Copy your active data regularly to ensure that the data is protected in case of a disaster.

If a file already exists in the active-data pool, the file is not copied unless the copy of the file in the active-data pool is marked damaged. However, a new copy is not created if the file in the primary storage pool is also marked damaged. In a random-access storage pool, neither cached copies of migrated files nor damaged primary files are copied.

If migration for a storage pool starts while active data is being copied, some files might be migrated before they are copied. For this reason, you should copy active data from storage pools that are higher in the migration hierarchy before copying active data from storage pools that are lower. Be sure a copy process is complete before beginning another.

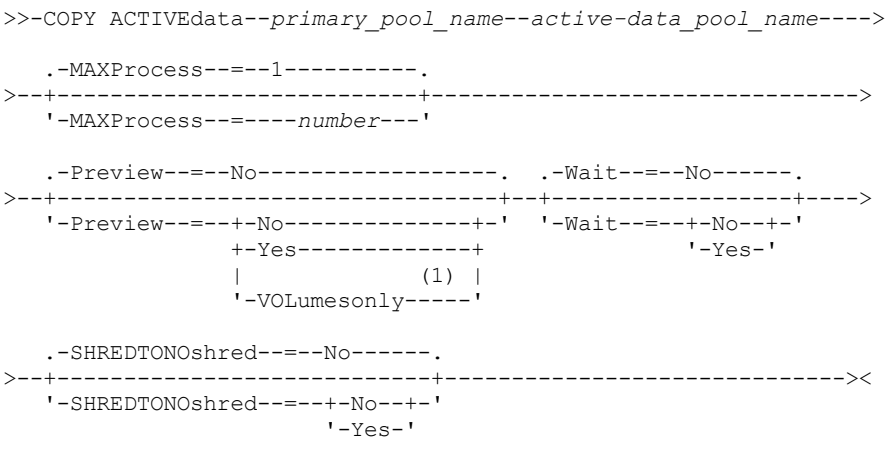
Remember:

- You can only copy active data from storage pools that have a data format of NATIVE or NONBLOCK.
- Issuing this command for a primary storage pool that is set up for data deduplication removes duplicate data, if the active-data pool is also set up for data deduplication.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the active-data pool from which active versions of backup data are being copied.

Syntax



Notes:

1. The VOLUMESONLY parameter applies to sequential-access storage pools only.

Parameters

primary_pool_name (Required)
: Specifies the primary storage pool.

active_data_pool_name (Required)
: Specifies the active-data pool.

MAXProcess
: Specifies the maximum number of parallel processes to use for copying files. This parameter is optional. Enter a value from 1 to 999. The default is 1.

  Using multiple, parallel processes may improve throughput for the COPY ACTIVEDATA command. The expectation is that the time needed to copy active data will be decreased by using multiple processes. However, when multiple processes are running, in some cases one or more of the processes might need to wait to use a volume that is already in use by a different COPY ACTIVEDATA process.

When determining this value, consider the number of logical and physical drives that can be dedicated to this operation. To access a sequential-access volume, the server uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other server and system activity, and also on the mount limits of the device classes for the sequential-access storage pools that are involved when copying active data.

Each process needs a mount point for active-data pool volumes, and, if the device type is not FILE, each process also needs a drive. If you are copying active data from a sequential-access storage pool, each process needs an additional mount point for primary storage pool volumes and, if the device type is not FILE, an additional drive. For example, suppose you specify a maximum of 3 processes to copy a primary sequential storage pool to an active-data pool of the same device class. Each process requires two mount points and two drives. To run all three processes, the device class must have a mount limit of at least six, and at least six mount points and six drives must be available.

To use the PREVIEW parameter, only one process is used, and no mount points or drives are needed.

Preview
Specifies whether you want to preview but not actually copy any active data. The preview displays the number of files and bytes to be copied and a list of the primary storage pool volumes that you must mount. This parameter is optional. The default is NO. Possible values are:

No
Specifies that active data will be copied.

Yes
Specifies that you want to preview the process but not copy any data.

VOLumesonly
Specifies that you want to preview the process only as a list of the volumes that must be mounted. This choice requires the least processing time.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. Possible values are:

No
Specifies that the server processes this command in the background.

You can continue with other tasks while the command is being processed. Messages created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files may have already been copied prior to the cancellation.

Yes
Specifies that the server performs this operation in the foreground. You must wait for the operation to complete before continuing with other tasks. The server displays the output messages to the administrative client when the operation completes.

You cannot specify WAIT=YES from the server console.

SHREDTONOshred
Specifies whether data should be copied from a primary storage pool that enforces shredding to an active-data pool that does not enforce shredding. This parameter is optional. The default value is NO. Possible values are:

No
Specifies that the server does not allow data to be copied from a primary storage pool that enforces shredding to an active-data pool that does not enforce shredding. If the primary storage pool enforces shredding and the active-data pool does not, the operation will fail.

Yes
Specifies that the server does allow data to be copied from a primary storage pool that enforces shredding to an active-data pool that does not enforce shredding. The data in the active-data pool will not be shredded when it is deleted.

Example: Copy primary storage pool data to active-data pool

Copy the active data from a primary storage pool named PRIMARY_POOL to the active-data pool named ACTIVEPOOL. Issue the command:

```
copy activedata primary_pool activepool
```

Related commands

Table 1. Commands related to COPY ACTIVEDATA

Command	Description
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT NODE	Restores client node information from external media.
IMPORT SERVER	Restores all or part of the server from external media.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY DOMAIN	Displays information about policy domains.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
UPDATE DOMAIN	Changes the attributes of a policy domain.
UPDATE STGPOOL	Changes the attributes of a storage pool.

COPY CLOPTSET (Copy a client option set)

Use this command to copy a client option set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax

```
>>-COPy CLOptset--current_option_set_name--new_option_set_name-><
```

Parameters

current_option_set_name (Required)
: Specifies the name of the client option set to be copied.

new_option_set_name (Required)
: Specifies the name of the new client option set. The maximum length of the name is 64 characters.

Example: Copy a client option set

Copy a client option set named ENG to a new client option set named ENG2.

```
copy cloptset eng eng2
```

Related commands

Table 1. Commands related to COPY CLOPTSET

Command	Description
DEFINE CLIENTOPT	Adds a client option to a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.

COPY DOMAIN (Copy a policy domain)

Use this command to create a copy of a policy domain.

The server copies the following information to the new domain:

- Policy domain description
- Policy sets in the policy domain (including the ACTIVE policy set, if a policy set is activated)
- Management classes in each policy set (including the default management class, if assigned)
- Copy groups in each management class

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-COPy DOmain--current_domain_name--new_domain_name----------><
```

Parameters

current_domain_name (Required)
: Specifies the policy domain to copy.

new_domain_name (Required)
: Specifies the name of the new policy domain. The maximum length of this name is 30 characters.

Example: Copy a policy domain to a new policy domain

Copy the STANDARD policy domain to a new policy domain, ENGPOLDOM, by entering the following command:

```
copy domain standard engpoldom
```

ENGPOLDOM now contains the standard policy set, management class, backup copy group, and archive copy group.

Related commands

Table 1. Commands related to COPY DOMAIN

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DEFINE MGMTCLASS	Defines a management class.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE COPYGROUP	Deletes a backup or archive copy group from a policy domain and policy set.
DELETE DOMAIN	Deletes a policy domain along with any policy objects in the policy domain.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY DOMAIN	Displays information about policy domains.
QUERY MGMTCLASS	Displays information about management classes.
QUERY POLICYSET	Displays information about policy sets.
REGISTER NODE	Defines a client node to the server and sets options for that user.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE DOMAIN	Changes the attributes of a policy domain.
UPDATE MGMTCLASS	Changes the attributes of a management class.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

COPY MGMTCLASS (Copy a management class)

Use this command to create a copy of a management class within the same policy set.

The server copies the following information to the new management class:

- Management class description
- Copy groups defined to the management class
- Any attributes for managing files for IBM Spectrum Protect™ for Space Management clients

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the new management class belongs.

Syntax

```
>>-COPy MGmtclass--domain_name--policy_set_name----------------->

>--current_class_name--new_class_name-------------------------><
```

Parameters

domain_name (Required)
Specifies the policy domain to which the management class belongs.
policy_set_name (Required)
Specifies the policy set to which the management class belongs.
current_class_name (Required)
Specifies the management class to copy.
new_class_name (Required)
Specifies the name of the new management class. The maximum length of this name is 30 characters.

Example: Copy a management class to a new management class

Copy the management class ACTIVEFILES to a new management class, FILEHISTORY. The management class is in policy set VACATION in the EMPLOYEE_RECORDS policy domain.

```
copy mgmtclass employee_records vacation
activefiles filehistory
```

Related commands

Table 1. Commands related to COPY MGMTCLASS

Command	Description
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.
QUERY POLICYSET	Displays information about policy sets.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE MGMTCLASS	Changes the attributes of a management class.

COPY POLICYSET (Copy a policy set)

Use this command to copy a policy set (including the ACTIVE policy set) within the same policy domain.

The server copies the following information to the new policy set:

- Policy set description
- Management classes in the policy set (including the default management class, if assigned)
- Copy groups in each management class

The policies in the new policy set do not take effect unless you make the new set the ACTIVE policy set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the new policy set belongs.

Syntax

```
>>-COPy POlicyset--domain_name--current_set_name--new_set_name-><
```

Parameters

domain_name (Required)
Specifies the policy domain to which the policy set belongs.

current_set_name (Required)
Specifies the policy set to copy.
new_set_name (Required)
Specifies the name of the new policy set. The maximum length of this name is 30 characters.

Example: Copy a policy set to a new policy set

Copy the policy set VACATION to the new policy set HOLIDAY in the EMPLOYEE_RECORDS policy domain.

```
copy policyset employee_records vacation holiday
```

Related commands

Table 1. Commands related to COPY POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE MGMTCLASS	Defines a management class.
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY POLICYSET	Displays information about policy sets.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

COPY PROFILE (Copy a profile)

Use this command on a configuration manager to copy a profile and all its associated object names to a new profile.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-COPy PROFIle--current_profile_name--new_profile_name-------><
```

Parameters

current_profile_name (Required)
Specifies the profile to copy.
new_profile_name (Required)
Specifies the name of the new profile. The maximum length of the profile name is 30 characters.

Example: Make a copy of a profile

Copy a profile named VAL to a new profile named VAL2.

```
copy profile val val2
```

Related commands

Table 1. Commands related to COPY PROFILE

Command	Description

Command	Description
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
LOCK PROFILE	Prevents distribution of a configuration profile.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY PROFILE	Displays information about configuration profiles.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

COPY SCHEDULE (Copy a client or an administrative command schedule)

Use this command to create a copy of a schedule.

The COPY SCHEDULE command takes two forms, depending on whether the schedule applies to client operations or administrative commands. The syntax and parameters for each form are defined separately.

Table 1. Commands related to COPY SCHEDULE

Command	Description
DEFINE ASSOCIATION	Associates clients with a schedule.
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
DELETE SCHEDULE	Deletes a schedule from the database.
QUERY SCHEDULE	Displays information about schedules.
UPDATE SCHEDULE	Changes the attributes of a schedule.

- COPY SCHEDULE (Create a copy of a schedule for client operations)
  Use the COPY SCHEDULE command to create a copy of a schedule for client operations. You can copy a schedule within a policy domain or from one policy domain to another policy domain. Use the DEFINE ASSOCIATION command to associate the new schedule with the client nodes.
- COPY SCHEDULE (Create a copy of a schedule for administrative operations)
  Use the COPY SCHEDULE command to create a copy of an administrative command schedule.

COPY SCHEDULE (Create a copy of a schedule for client operations)

Use the COPY SCHEDULE command to create a copy of a schedule for client operations. You can copy a schedule within a policy domain or from one policy domain to another policy domain. Use the DEFINE ASSOCIATION command to associate the new schedule with the client nodes.

Privilege class

To copy a client schedule, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which you are copying the schedule.

Syntax

```
>>-COPy SCHedule--current_domain_name--current_sched_name------->

                    .-current_sched_name-.
>--new_domain_name--+--------------------+---------------------->
                    '-new_sched_name-----'

   .-REPlace--=--No------.
>--+---------------------+-------------------------------------><
   '-REPlace--=--+-No--+-'
                 '-Yes-'
```

Parameters

current_domain_name (Required)
: Specifies the name of the policy domain that contains the schedule you want to copy.

current_sched_name (Required)
: Specifies the name of the schedule you want to copy.

new_domain_name (Required)
: Specifies the name of a policy domain to which you want to copy the new schedule.

new_sched_name
: Specifies the name of the new schedule. You can specify up to 30 characters for the name.

  If you do not specify this name, the name of the original schedule is used.

  If the schedule name is already defined in the policy domain, you must specify REPLACE=YES, or the command fails.

REPlace
: Specifies whether to replace a client schedule. The default is NO. The values are:

  No
  : Specifies that a client schedule is not replaced.

  Yes
  : Specifies that a client schedule is replaced.

Example: Copy a schedule from one policy domain to another

Copy the WEEKLY_BACKUP schedule that belongs to policy domain EMPLOYEE_RECORDS to the PROG1 policy domain and name the new schedule WEEKLY_BACK2. If there is already a schedule with this name defined in the PROG1 policy domain, do not replace it.

```
copy schedule employee_records weekly_backup
prog1 weekly_back2
```

COPY SCHEDULE (Create a copy of a schedule for administrative operations)

Use the COPY SCHEDULE command to create a copy of an administrative command schedule.

Privilege class

To copy an administrative command schedule, you must have system privilege.

Syntax

```
>>-COPy SCHedule--current_sched_name--new_sched_name------------>
```

```
                              .-REPlace--=--No------.
>--Type--=--Administrative--+---------------------+------------><
                              '-REPlace--=--+-No--+-'
                                            '-Yes-'
```

Parameters

current_schedule_name (Required)
: Specifies the name of the schedule you want to copy.

new_schedule_name (Required)
: Specifies the name of the new schedule. You can specify up to 30 characters for the name.

  If the schedule name is already defined, you must specify REPLACE=YES, or the command fails.

Type=Administrative
: Specifies that an administrative command schedule is to be copied.

REPlace
: Specifies whether to replace an administrative command schedule. The default is NO. The values are:

  No
  : Specifies that an administrative command schedule is not replaced.

  Yes
  : Specifies that an administrative command schedule is replaced.

Example: Copy an administrative command schedule to another schedule

Copy the administrative command schedule, DATA_BACKUP and name the schedule DATA_ENG. If there is already a schedule with this name, replace it.

```
copy schedule data_backup data_eng
type=administrative replace=yes
```

COPY SCRIPT (Copy an IBM Spectrum Protect script)

Use this command to copy an existing IBM Spectrum Protect™ script to a new script with a different name.

Privilege class

To issue this command, you must have operator, policy, storage, or system privilege.

Syntax

```
>>-COPy SCRipt--current_script_name--new_script_name ----------><
```

Parameters

current_script_name (Required)
: Specifies the name of the script you want to copy.

new_script_name (Required)
: Specifies the name of the new script. You can specify up to 30 characters for the name.

Example: Make a copy of a script

Copy script TESTDEV to a new script and name it ENGDEV.

```
copy script testdev engdev
```

Related commands

Table 1. Commands related to COPY SCRIPT

Command	Description
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
QUERY SCRIPT	Displays information about scripts.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

COPY SERVERGROUP (Copy a server group)

Use this command to create a copy of a server group.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-COPy SERVERGroup--current_group_name--new_group_name-------><
```

Parameters

current_group_name (Required)
: Specifies the server group to copy.

new_group_name (Required)
: Specifies the name of the new server group. The maximum length of this name is 64 characters.

Example: Make a copy of a server group

Copy the server group GRP_PAYROLL to the new group HQ_PAYROLL.

```
copy servergroup grp_payroll hq_payroll
```

Related commands

Table 1. Commands related to COPY SERVERGROUP

Command	Description
DEFINE GRPMEMBER	Defines a server as a member of a server group.
DEFINE SERVER	Defines a server for server-to-server communications.
DEFINE SERVERGROUP	Defines a new server group.
DELETE GRPMEMBER	Deletes a server from a server group.
DELETE SERVER	Deletes the definition of a server.
DELETE SERVERGROUP	Deletes a server group.
MOVE GRPMEMBER	Moves a server group member.
QUERY SERVER	Displays information about servers.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVER	Updates information about a server.
UPDATE SERVERGROUP	Updates a server group.

DEACTIVATE DATA (Deactivate data for a client node)

Use this command to specify that active data that was backed up for an application client node before a specified date is no longer needed. The command marks the data as inactive so it can be deleted according to your data retention policies.

Restriction: The DEACTIVATE DATA command applies only to application clients that protect Oracle databases.

When you issue the DEACTIVATE DATA command, all active backup data that was stored before the specified date becomes inactive. The data can no longer be retrieved, and is deleted when it expires.

The DEACTIVATE DATA command affects only the files that were copied to the server before the specified date and time. Files that were copied after the specified date are still accessible, and the client can still access the server.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEACtivate DAta--node_name--TODate--=--date------------------>

   .-TOTime--=--23:59:59-.  .-Wait--=--No------.
>--+---------------------+--+------------------+--------------><
   '-TOTime--=--time-----'  '-Wait--=--+-No--+-'
                                       '-Yes-'
```

Parameters

node_name (Required)

Specifies the name of an application client node whose data is to be deactivated.

TODate (Required)

Specifies the date to use to select the backup files to deactivate. IBM Spectrum Protect™ deactivates only those files with a date on or before the date you specify. You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	01/23/2014
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–30 **or** –30. To deactivate files that are 30 or more days old, you can specify TODAY-30 or -30.
EOLM	End of last month. The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To deactivate files that were active a day before the last day of the previous month.
BOTM	Beginning of this month. The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To deactivate files that were active on the 10th day of the current month.

TOTime

Specifies that you want to deactivate files that were created on the server before this time on the specified date. This parameter is optional. The default is the end of the day (23:59:59). Specify the time by using one of the following values:

Value	Description	Example

Value	Description	Example
HH:MM:SS	A specific time on the specified date	12:30:22
NOW	The current time on the specified date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified date	NOW+03:00 **or** +03:00. If you issue the DEACTIVATE DATA command at 9:00 with TOTIME=NOW+03:00 or TOTIME=+03:00, IBM Spectrum Protect deactivates files that were put on the server at 12:00 or earlier on the specified date.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified date	NOW-03:30 **or** -03:30. If you issue the DEACTIVATE DATA command at 9:00 with TOTIME=NOW-3:30 or TOTIME=-3:30, IBM Spectrum Protect deactivates files that were put on the server at 5:30 or earlier on the specified date.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is NO. Specify the following values:

No

The server processes this command in the background and you can continue with other tasks while the command is processing. Messages that are related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged.

Yes

The server processes this command in the foreground. The operation must complete before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.

Restriction: You cannot specify WAIT=YES from the server console.

Example: Deactivate data for a data protection client node

The client node BANDIT is an IBM Spectrum Protect for Databases: Data Protection for Oracle application client. All of the backup data is active, and so all of the backup data is retained. The following command deactivates data that was backed up before January 3, 2014, so it can be deleted when it expires.

```
deactivate data bandit todate=01/23/2014
```

To periodically deactivate data so it can be deleted when it expires, you might run the following command from within a client schedule.

```
deactivate data bandit todate=today
```

Related commands

Table 1. Commands related to DEACTIVATE DATA

Command	Description
DECOMMISSION NODE	Decommissions an application or system.
DECOMMISSION VM	Decommissions a virtual machine.

DECOMMISSION commands

Use the DECOMMISSION commands to remove client nodes from the production environment. Client nodes include applications, systems, and virtual machines.

- DECOMMISSION NODE (Decommission an application or system)
- DECOMMISSION VM (Decommission a virtual machine)

DECOMMISSION NODE (Decommission an application or system)

Use this command to remove an application or system client node from the production environment. Any backup data that is stored for the client node expires according to policy settings unless you explicitly delete the data.

Attention: This action cannot be reversed and causes deletion of data. Although this command does not delete the client node definition until after its data expires, you cannot recommission the client node. After you issue this command, the client node cannot access the server and its data is not backed up. The client node is locked, and can be unlocked only to restore files. File spaces that belong to the client node, and the client node itself, are eventually removed.
By using this command, you can decommission the following types of client nodes:

Application client nodes
: Application client nodes include email servers, databases, and other applications. For example, any of the following applications can be an application client node:

  - IBM Spectrum Protect™ Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

System client nodes
: System client nodes include workstations, network-attached storage (NAS) file servers, and API clients.

When a client node is no longer needed in the production environment, you can issue this command to initiate a gradual, controlled decommission operation. The command completes the following actions:

- Deletes all schedule associations for the client node. Schedules are no longer run on the client node. This action is equivalent to issuing the DELETE ASSOCIATION command for every schedule with which the client node is associated.
- Prevents the client from accessing the server. This action is equivalent to issuing the LOCK NODE command.

After the command finishes, client node data is no longer backed up to the server. Data that was backed up before the client node was decommissioned is not immediately deleted from the server. However, all backup file versions, including the most recent backup, are now inactive copies. The client files are retained on the server according to your storage management policies.

After all data retention periods expire, and all client backup and archive file copies are removed from server storage, IBM Spectrum Protect deletes the file spaces that belong to the decommissioned node. This action is equivalent to issuing the DELETE FILESPACE command.

After the file spaces for the decommissioned node are deleted, the node definition is deleted from the server. This action is equivalent to issuing the REMOVE NODE command.

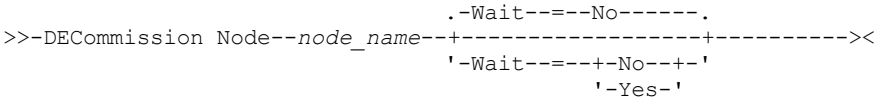
After you decommission a client node, but before it is removed from the server, you can use the QUERY NODE command to verify that the client node is decommissioned.

Restriction: You cannot decommission a client node that is configured for replication. You can determine a client node's replication state by using the QUERY NODE command. If a client node is configured for replication, you can remove the client node from replication by using the REMOVE REPLNODE command.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

node_name (Required)
Specifies the name of the client node to be decommissioned.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is NO. You can specify the following values:

No
The server processes this command in the background and you can continue with other tasks while the command is processing. Messages that are related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged.

Yes
The server processes this command in the foreground. The operation must complete before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.

Restriction: You cannot specify WAIT=YES from the server console.

Example: Decommission a client node

Decommission the client node CODY.

```
decommission node cody
```

Related commands

Table 1. Commands related to DECOMMISSION NODE

Command	Description
DECOMMISSION VM	Decommissions a virtual machine.
DEACTIVATE DATA	Deactivates data for a client node.

DECOMMISSION VM (Decommission a virtual machine)

Use this command to remove an individual virtual machine within a data center node. The file space that represents the virtual machine is deleted from the server only after its backup data expires.

Attention: This command cannot be reversed and causes deletion of data. Although this command does not delete the virtual machine file space until after its data expires, you cannot recommission the virtual machine.

When a virtual machine is no longer needed in your production environment, you can issue this command to initiate a staged removal of the virtual machine file space from the server. The DECOMMISSION VM command marks all data that was backed up for the virtual machine as inactive, so it can be deleted according to your data retention policies. After all data that was backed up for the virtual machine expires, the file space that represents the virtual machine is deleted. The DECOMMISSION VM command affects only the virtual machine that you identify. The data center node, and the other virtual machines that are hosted by the data center node are not affected.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DECommission VM--node_name--vm_name--------------------------->

                              .-Wait--=--No------.
>--+-----------------------+--+------------------+-------------><
   '-NAMEType--=----FSID---'  '-Wait--=--+-Yes-+-'
                                         '-No--'
```

Parameters

node_name (Required)
Specifies the name of the data center node that hosts the virtual machine to be decommissioned.

vm_name (Required)
Identifies the file space that represents the virtual machine to be decommissioned. Each virtual machine that is hosted by a data center node is represented as a file space.

If the name includes one or more spaces, you must enclose the name in double quotation marks when you issue the command.

By default, the server interprets the file space name that you enter by using the server code page and also attempts to convert the file space name from the server code page to the UTF-8 code page. Conversion might fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

If the name of the virtual machine is a non-English-language name, this parameter must specify the file space ID (FSID). By specifying the NAMEType parameter, you can instruct the server to interpret the file space name by its file space ID (FSID) instead.

NAMEType
Specify how you want the server to interpret the file space name that you enter to identify the virtual machine. This parameter is useful when the server has clients with Unicode support. You can specify the following value:

FSID
The server interprets the file space name by its file space ID (FSID).

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is No. You can specify the following values:

No
The server processes this command in the background and you can continue with other tasks while the command is processing. Messages that are related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged.

Yes
The server processes this command in the foreground. The operation must complete before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.

Restriction: You cannot specify WAIT=YES from the server console.

Examples: Decommission a virtual machine

Decommission the virtual machine CODY.

```
decommission vm dept06node cody
```

Decommission the virtual machine CODY 2.

```
decommission vm dept06node "cody 2"
```

Decommission a virtual machine by specifying its file space ID.

```
decommission vm dept06node 7 nametype=fsid
```

Related commands

Table 1. Commands related to DECOMMISSION VM

Command	Description
DECOMMISSION NODE	Decommissions an application or system.
DEACTIVATE DATA	Deactivates data for a client node.

DEFINE commands

Use the DEFINE commands to create IBM Spectrum Protect™ objects.

- DEFINE ALERTTRIGGER (Define an alert trigger)
- DEFINE ASSOCIATION (Associate client nodes with a schedule)
- DEFINE BACKUPSET (Define a backup set)
- DEFINE CLIENTACTION (Define a one-time client action)
- DEFINE CLIENTOPT (Define an option to an option set)
- DEFINE CLOPTSET (Define a client option set name)
- DEFINE COLLOCGROUP (Define a collocation group)
- DEFINE COLLOCMEMBER (Define collocation group member)
- DEFINE COPYGROUP (Define a copy group)
- DEFINE DATAMOVER (Define a data mover)
- DEFINE DEVCLASS (Define a device class)
- DEFINE DOMAIN (Define a new policy domain)
- DEFINE DRIVE (Define a drive to a library)
- DEFINE EVENTSERVER (Define a server as the event server)
- DEFINE GRPMEMBER (Add a server to a server group)
- DEFINE LIBRARY (Define a library)
- DEFINE MACHINE (Define machine information for disaster recovery)
- DEFINE MACHNODEASSOCIATION (Associate a node with a machine)
- DEFINE MGMTCLASS (Define a management class)
- DEFINE NODEGROUP (Define a node group)
- DEFINE NODEGROUPMEMBER (Define node group member)
- DEFINE PATH (Define a path)
- DEFINE POLICYSET (Define a policy set)
- DEFINE PROFASSOCIATION (Define a profile association)
- DEFINE PROFILE (Define a profile)
- DEFINE RECMEDMACHASSOCIATION (Associate recovery media with a machine)
- DEFINE RECOVERYMEDIA (Define recovery media)
- DEFINE SCHEDULE (Define a client or an administrative command schedule)
- DEFINE SCRIPT (Define an IBM Spectrum Protect script)
- DEFINE SERVER (Define a server for server-to-server communications)
- DEFINE SERVERGROUP (Define a server group)
- DEFINE SPACETRIGGER (Define the space trigger)
- DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)
- DEFINE STGRULE (Define a rule for auditing storage pools)
- DEFINE STGRULE (Define a rule for generating data deduplication statistics)
- DEFINE STGRULE (Define a rule for reclaiming cloud containers)
- DEFINE STGRULE (Define a storage rule for tiering)
- DEFINE STGPOOL (Define a storage pool)
- DEFINE STGPOOLDIRECTORY (Define a storage pool directory)
- DEFINE SUBSCRIPTION (Define a profile subscription)
- DEFINE VIRTUALFSMAPPING (Define a virtual file space mapping)
- DEFINE VOLUME (Define a volume in a storage pool)

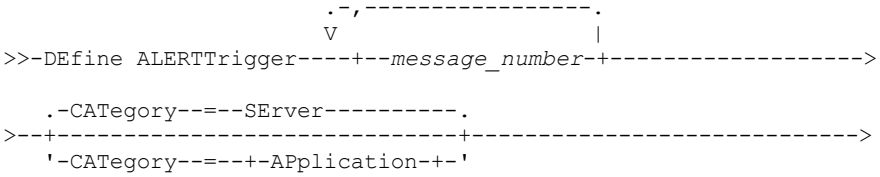
DEFINE ALERTTRIGGER (Define an alert trigger)

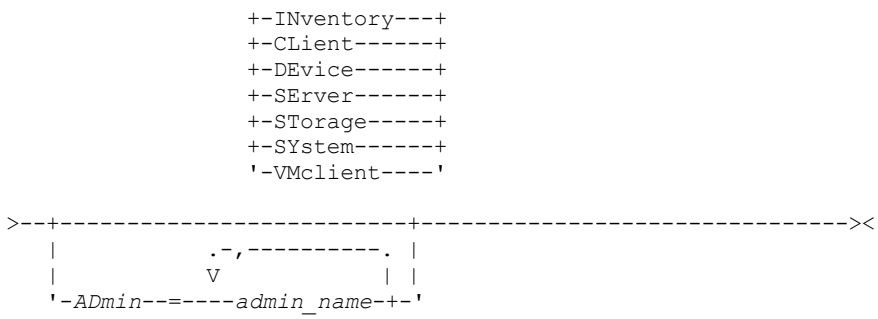
Use this command to trigger an alert whenever a server issues a specific error message. You can define a message number to be an alert trigger, assign it to a category, or specify administrators who can be notified of the alert by email.

Privilege class

To issue this command, you must have system privilege.

Syntax





Parameters

message_number (Required)
: Specifies the message number that you want to associate with the alert trigger. Specify multiple message numbers, which are separated by commas, and no intervening spaces. Message numbers are a maximum of eight characters in length.

CATegory
: Specifies the category type for the alert, which is determined by the message types. The default value is SERVER.
Note: Changing the category of an alert trigger does not change the category of existing alerts on the server. New alerts are categorized with the new category.
Specify one of the following values:

  APplication
  : Alert is classified as application category. For example, you can specify this category for messages that are associated with application (TDP) clients.

  INventory
  : Alert is classified as inventory category. For example, you can specify this category for messages that are associated with the database, active log file, or archive log file.

  CLient
  : Alert is classified as client category. For example, you can specify this category for messages that are associated with general client activities.

  DEvice
  : Alert is classified as device category. For example, you can specify this category for messages that are associated with device classes, libraries, drives, or paths.

  SErver
  : Alert is classified as general server category. For example, you can specify this category for messages that are associated with general server activities or events.

  STorage
  : Alert is classified as storage category. For example, you can specify this category for messages that are associated with storage pools.

  SYstems
  : Alert is classified under system clients category. For example, you can specify this category for messages that are associated with system backup and archive or hierarchical storage management (HSM) backup-archive clients.

  VMclient
  : Alert is classified under VMclient category. For example, you can specify this category for messages that are associated with virtual machine clients.

ADmin
: This optional parameter specifies the name of the administrator who receives email notification of this alert. The alert trigger is defined successfully even if no administrator names are specified.

Assign two message numbers to an alert

Issue the following command to specify that you want two message numbers to trigger an alert:

```
define alerttrigger ANR1067E,ANR1073E
```

Assign a message number to an alert and email two administrators

Issue the following command to specify the message numbers that you want to trigger an alert and have them sent by email to two administrators:

```
define alerttrigger ANR1067E,ANR1073E ADmin=BILL,DJADMIN
```

Related commands

Table 1. Commands related to DEFINE ALERTTRIGGER

Command	Description
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

DEFINE ASSOCIATION (Associate client nodes with a schedule)

Use this command to associate one or more clients with a schedule. You must assign a client node to the policy domain to which a schedule belongs. Client nodes process operations according to the schedules associated with the nodes.

Note:

1. IBM Spectrum Protect™ cannot run multiple schedules concurrently for the same client node.
2. In a macro, the server may stall if some commands (such as REGISTER NODE and DEFINE ASSOCIATION) are not committed as soon as you issue them. You could follow each command in a macro with a COMMIT command. However, a simpler solution is to include the -ITEMCOMMIT option with the DSMADMC command.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege
- Restricted policy privilege for the policy domain to which the schedule belongs

Syntax

```
>>-DEFine ASSOCiation--domain_name--schedule_name--------------->

   .-,---------.
   V           |
>----node_name-+-----------------------------------------------><
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the schedule belongs.

schedule_name (Required)
: Specifies the name of the schedule that you want to associate with one or more clients.

node_name (Required)
: Specifies the name of a client node or a list of client nodes to associate with the specified schedule. Use commas to separate the items in the list. Do not leave spaces between the items and commas. You can use a wildcard character to specify a name. The command will not associate a listed client to the schedule if:

  - The client is already associated with the specified schedule.
  - The client is not assigned to the policy domain to which the schedule belongs.

- The client is a NAS node name. All NAS nodes are ignored.

Example: Associate client nodes with a schedule

Associate the client nodes SMITH or JOHN with the WEEKLY_BACKUP schedule. The associated clients are assigned to the EMPLOYEE_RECORDS policy domain.

```
define association employee_records
weekly_backup smith*,john*
```

Example: Associate client nodes with a schedule

Associate the client nodes JOE, TOM, and LARRY with the WINTER schedule. The associated clients are assigned to the EMPLOYEE_RECORDS policy domain; however, the client JOE is already associated with the WINTER schedule.

```
define association employee_records
winter joe,tom,larry
```

Related commands

Table 1. Commands related to DEFINE ASSOCIATION

Command	Description
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
DELETE ASSOCIATION	Deletes the association between clients and a schedule.
DELETE SCHEDULE	Deletes a schedule from the database.
QUERY ASSOCIATION	Displays the clients associated with one or more schedules.
REGISTER NODE	Defines a client node to the server and sets options for that user.

DEFINE BACKUPSET (Define a backup set)

Use this command to define a client backup set that was previously generated on one server and make it available to the server that is running this command. The client node has the option of restoring the backup set from the server that is running this command rather than the one on which the backup set was generated.

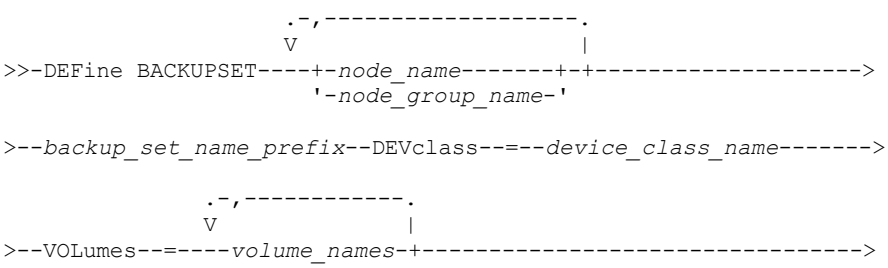
Any backup set generated on one server can be defined to another server when the servers share a common device type. The level of the server to which the backup set is being defined must be equal to or greater than the level of the server that generated the backup set.

You can also use the DEFINE BACKUPSET command to redefine a backup set that was deleted on a server.

Privilege class

If the REQSYSAUTHOUTFILE server option is set to YES (the default), the administrator must have system privilege. If the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax



```
   .-RETention--=--365---------.
>--+---------------------------+------------------------------->
   '-RETention--=--+-days----+-'
                   '-NOLimit-'

>--+-----------------------------+----------------------------->
   '-DESCription--=--description-'

   .-WHEREDATAType--=--ALL-----------.
>--+---------------------------------+------------------------->
   |                    .-,---------. |
   |                    V           | |
   '-WHEREDATAType--=-----+-FILE--+-+-'
                          '-IMAGE-'

>--+----------------------+--+----------------------------+--><
   '-TOC--=--+-PREFERRED-+-'  '-TOCMGmtclass--=--class_name-'
             +-YES-------+
             '-NO--------'
```

Parameters

node_name or node_group_name (Required)
: Specifies the name of the client nodes or node groups whose data is contained in the specified backup set volumes. To specify multiple node and node group names, separate the names with commas and no intervening spaces. Node names can contain wildcard characters, but node group names cannot. If the backup set volumes contain backup sets from multiple nodes, every backup set whose node name matches one of the specified node names is defined. If the volumes contain a backup set for a node that is not currently registered, the DEFINE BACKUPSET command does not define the backup set for that node.

backup_set_name_prefix (Required)
: Specifies the name of the backup set to define to this server. The maximum length of the name is 30 characters.

  When you select a name, IBM Spectrum Protect™ adds a suffix to construct the backup set name. For example, if you name your backup set *mybackupset*, IBM Spectrum Protect adds a unique number such as 3099 to the name. Your backup set name is then identified as *mybackupset.3099*. To later display information about this backup set, you can include a wildcard with the name, such as *mybackupset** or you can specify the fully qualified name, such as *mybackupset.3099*.

  If the backup set volumes contain backup sets for multiple nodes, then backup sets are defined for each of the nodes by using the same backup set name prefix and suffix.

DEVclass (Required)
: Specifies the device class name for the volumes from which the backup set is read.
  Note: The device type that is associated with the device class you specify must match the device class with which the backup set was originally generated.

VOLumes (Required)
: Specifies the names of the volumes that are used to store the backup set. You can specify multiple volumes by separating the names with commas and no intervening spaces. The volumes that you specify must be available to the server that is defining the backup set.
  Note: The volumes that you specify must be listed in the order they were created, or the DEFINE BACKUPSET command fails.
  The server does not verify that every volume specified for a multiple-volume backup set contains part of the backup set. The first volume is always checked, and in some cases extra volumes are also checked. If these volumes are correct, the backup set is defined and all of the volumes that are listed in the command are protected from being overwritten. If a volume that contains part of the backup set is not listed in the command, the volume is not protected and can potentially be overwritten during normal server operations.
  Note: By default, the server attempts to create a table of contents when a backup set is defined. If an incorrect volume is specified, or if volumes are not listed in the correct order, the table of contents creation fails. If this failure occurs, check the volume list in the command and consider using the QUERY BACKUPSETCONTENTS command to verify the contents of the backup set.

RETention
: Specifies the number of days that the backup set is retained on the server. You can specify an integer 0 - 30000. The default is 365 days. The values are:

  days

Specifies the number of days to retain the backup set on the server.

NOLimit
Specifies that the backup set must be retained on the server indefinitely.

If you specify NOLIMIT, IBM Spectrum Protect retains the volumes that contain the backup set forever, unless a user or administrator deletes the volumes from server storage.

DESCription
Specifies the description to associate with the backup set that belongs to the client node. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

WHEREDATAType
Specifies the backup sets containing the specified types of data are to be defined. This parameter is optional. The default is that backup sets for all types of data (file level, image, and application) are to be defined. To specify multiple data types, separate the data types with commas and no intervening spaces. Possible values are:

ALL
Specifies that backup sets for all types of data (file level, image, and application) are to be defined. ALL is the default value.

FILE
Specifies that a file level backup set is to be defined. File level backup sets contain files and directories that are backed up by the backup client.

IMAGE
Specifies that an image backup set is to be defined. Image backup sets contain images that are created by the backup-archive client BACKUP IMAGE command.

TOC
Specifies whether a table of contents (TOC) must be created for the file level backup set when it is defined. The TOC parameter is ignored when you define image and application data backup sets because a table of contents is always created for these backup sets.
Consider the following in determining whether you want to create a table of contents:

- If a table of contents is created, you can use the IBM Spectrum Protect web backup-archive client to examine the entire file system tree and choose files and directories to restore. Creation of a table of contents requires that you define the TOCDESTINATION attribute in the backup copy group for the management class that is specified by the TOCMGMTCLASS parameter. To create a table of contents extra processing, storage pool space, and possibly a mount point during the backup set operation is required.
- If a table of contents is not saved for a backup set, you can still restore individual files or directory trees by using the backup-archive client RESTORE BACKUPSET command if you know the fully qualified name of each file or directory to be restored.

This parameter is optional. The default value is Preferred. Possible values are:

No
Specifies that table of contents information is not saved for file level backup sets.

Preferred
Specifies that table of contents information must be saved for file level backup sets. However, a backup set does not fail just because an error occurs during creation of the table of contents.

Yes
Specifies that table of contents information must be saved for each file level backup set. A backup set fails if an error occurs during creation of the table of contents.

TOCMGmtclass
Specifies the name of the management class to which the table of contents must be bound. If you do not specify a management class, the table of contents is bound to the default management class for the policy domain to which the node is assigned. In this case, creation of a table of contents requires that you define the TOCDESTINATION attribute in the backup copy group for the specified management class.

Example: Define a backup set

Define the PERS_DATA backup set that belongs to client node JANE to the server that is running this command. Retain the backup set on the server for 50 days. Specify that volumes VOL001 and VOL002 contain the data for the backup set. The volumes are to be read by a device that is assigned to the AGADM device class. Include a description.

```
define backupset jane pers_data devclass=agadm
volumes=vol1,vol2 retention=50
description="sector 7 base image"
```

Related commands

Table 1. Commands related to DEFINE BACKUPSET

Command	Description
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE NODEGROUP	Deletes a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
QUERY BACKUPSET	Displays backup sets.
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

DEFINE CLIENTACTION (Define a one-time client action)

Use this command to schedule one or more clients to process a command for a one-time action.

The server automatically defines a schedule and associates the client node to the schedule. The server assigns the schedule priority 1, sets the PERUNITS to ONETIME, and determines the number of days to keep the schedule active. The number of days is based on the value set with the SET CLIENTACTDURATION command.

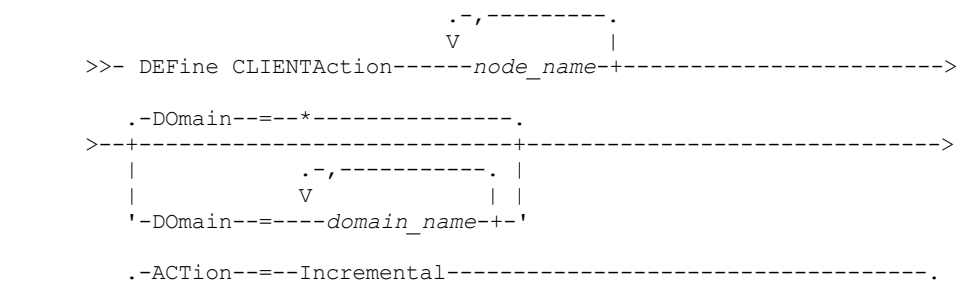
How quickly the client processes this command depends on whether the scheduling mode for the client is set to server-prompted or client-polling. The client scheduler must be started on the client workstation in order for the server to process the schedule.

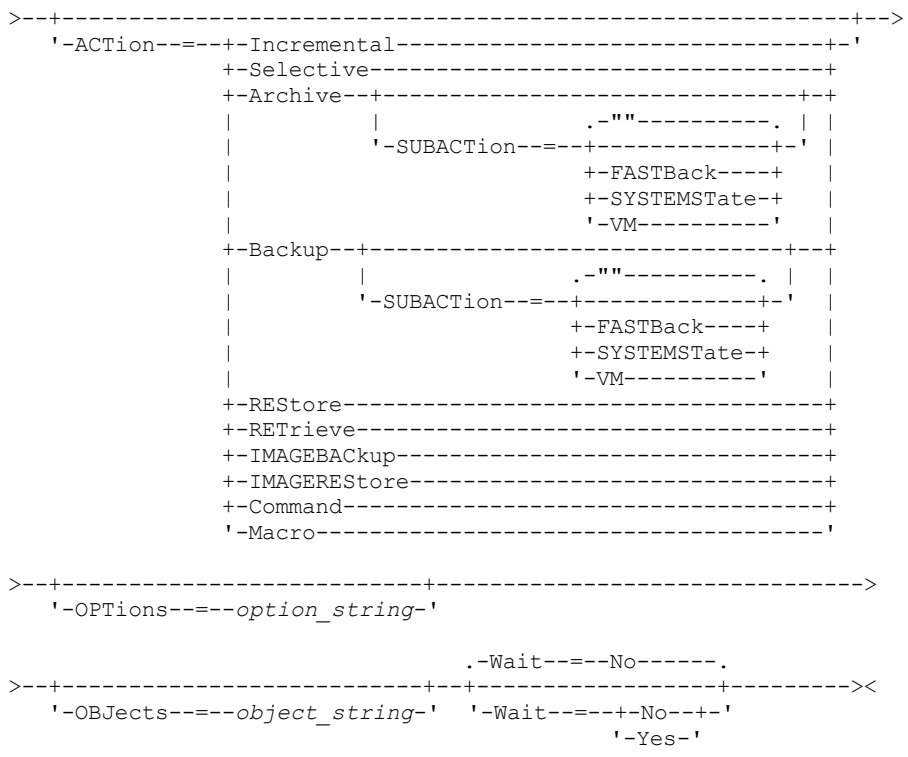
Remember: The start of the IBM Spectrum Protect™ scheduler depends on the processing of other threads in the server and other processes on the IBM Spectrum Protect server host system. The amount of time it takes to start the scheduler also depends on network traffic and how long it takes to open a socket, to connect with the IBM Spectrum Protect client, and to receive a response from the client. In general, the greater the processing and connectivity requirements on the IBM Spectrum Protect server and client, the longer it can take to start the scheduler.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy for the policy domain to which the schedule belongs.

Syntax





Parameters

node_name (Required)
Specifies the name of the client node that will process the schedule associated with the action. If you specify multiple node names, separate the names with commas; do not use intervening spaces. You can use the asterisk wildcard character to specify multiple names.

DOmain
Specifies the list of policy domains used to limit the list of client nodes. Only client nodes that are assigned to one of the specified policy domains will be scheduled. All clients assigned to a matching domain will be scheduled. Separate multiple domain names with commas and no intervening spaces. If you do not specify a value, all policy domains will be included in the list.

ACTion
Specifies the action that occurs when this schedule is processed. Possible values are:

Incremental
Specifies that the schedule backs up all files that are new or that have changed since the last incremental backup. Incremental also backs up any file for which all existing backups might have expired.

Selective
Specifies that the schedule backs up only files that are specified with the OBJECTS parameter.

Archive
Specifies that the schedule archives files that are specified with the OBJECTS parameter.

Backup
Specifies that the schedule backs up files that are specified with the OBJECTS parameter.

REStore
Specifies that the schedule restores files that are specified with the OBJECTS parameter.

When you specify ACTION=RESTORE for a scheduled operation, and the REPLACE option is set to PROMPT, no prompting occurs. If you set the option to PROMPT, the files are skipped.

If you specify a second file specification, this second file specification acts as the restore destination. If you need to restore multiple groups of files, schedule one for each file specification that you need to restore.

RETrieve
Indicates that the schedule retrieves files that are specified with the OBJECTS parameter.
Remember: A second file that is specified acts as the retrieve destination. If you need to retrieve multiple groups of files, create a separate schedule for each group of files.

IMAGEBACkup

Specifies that the schedule backs up logical volumes that are specified with the OBJECTS parameter.

IMAGEREStore
: Specifies that the schedule restores logical volumes that are specified with the OBJECTS parameter.

Command
: Specifies that the schedule processes a client operating system command or script that is specified with the OBJECTS parameter.

Macro
: Specifies that a client processes a macro whose file name is specified with the OBJECTS parameter.

SUBACTion
: You can specify one of the following values:

  ""
  : When a null string (two double quotes) is specified with ACTION=BACKUP the backup is an incremental.

  FASTBAck
  : Specifies that a FastBack client operation that is identified by the ACTION parameter is to be scheduled for processing. The ACTION parameter must be either ARCHIVE or BACKUP.

  SYSTEMSTate
  : Specifies that a client Systemstate backup is scheduled.

  VApp
  : Specifies that a client vApp backup is scheduled. A vApp is a collection of pre-deployed virtual machines.

  VM
  : Specifies that a client VMware backup operation is scheduled.

OPTions
: Specifies the client options that you specify to the scheduled command at the time the schedule is processed. This parameter is optional.
Only those options that are valid on the scheduled command can be specified for this parameter. Refer to the appropriate client manual for information about options that are valid from the command line. All options described there as valid only on the initial command line result in an error or are ignored when running the schedule from the server. For example, do not include the following options because they have no effect when the client processes the scheduled command:

  - MAXCMDRETRIES
  - OPTFILE
  - QUERYSCHEDPERIOD
  - RETRYPERIOD
  - SCHEDLOGNAME
  - SCHEDMODE
  - SERVERNAME
  - TCPCLIENTADDRESS
  - TCPCLIENTPORT

  Windows When you define a scheduler service by using the DSMCUTIL command or the backup-archive client GUI wizard, you specify an options file. You cannot override the options in that options file by issuing the scheduled command. You must modify the options in your scheduler service.

  If the option string contains multiple options or options with embedded spaces, surround the entire option string with one pair of apostrophes. Enclose individual options that contain spaces in quotation marks. A leading minus sign is required in front of the option. Errors can occur if the option string contains spaces that are not quoted correctly.

  The following examples show how to specify some client options:

  - To specify `subdir=yes` and `domain all-local -systemobject`, enter:
    - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
  - To specify `domain all-local -c: -d:`, enter:
    - `options='-domain="all-local -c: -d:"'`

  Windows Tip:

  For Windows clients running in batch mode, if the use of quotation marks is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

  - Processing a series of commands from the administrative client
  - Processing individual commands from the administrative client

OBJects

Specifies the objects for which the specified action is performed. Use a single space between each object. This parameter is required except when ACTION=INCREMENTAL. If the action is a backup, archive, retrieve, or restore operation, the objects are file spaces, directories, or logical volumes. If the action is to run a command or macro, the object is the name of the command or macro to run.

When you specify ACTION=INCREMENTAL without specifying a value for this parameter, the scheduled command is invoked without specified objects and attempts to process the objects as defined in the client option file. To select all file spaces or directories for an action, explicitly list them in the object string. Entering only an asterisk in the object string causes the backup to occur only for the directory where the scheduler was started.

Important:

- If you specify a second file specification, and it is not a valid destination, you receive this error:

  ```
  ANS1082E Invalid destination file specification <filespec> entered.
  ```

- If you specify more than two file specifications, you receive this error:

  ```
  ANS1102E Excessive number of command line arguments passed to the
  program!
  ```

When you specify ACTION=ARCHIVE, INCREMENTAL, or SELECTIVE for this parameter, you can list a maximum of twenty (20) file specifications.

Enclose the object string in double quotes if it contains blank characters (spaces), and then surround the double quotes with single quotes. If the object string contains multiple file names, enclose each file name with its own pair of double quotes, then surround the entire string with one pair of single quotes. Errors can occur if file names contain a space that is not quoted correctly.

Windows If you are using characters that have a special meaning for Windows users, such as commas, surround the entire argument in two pairs of double quotes, then surround the entire string with single quotes. The following examples show you how to specify some file names:

- To specify C:\FILE 2, D:\GIF FILES, and E:\MY TEST FILE, enter:
  - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
- To specify D:\TEST FILE, enter:
  - `OBJECTS='"D:\TEST FILE"'`
- To specify D:TEST,FILE:
  - `OBJECTS='""D:\TEST,FILE""'`

AIX Linux The following examples show how to specify some file names:

- To specify /home/file 2, /home/gif files, and /home/my test file, enter:
  - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
- To specify /home/test file, enter:
  - `OBJECTS='"/home/test file"'`

Windows Tip:

For Windows clients running in batch mode, if the use of double quotes is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

- Processing a series of commands from the administrative client
- Processing individual commands from the administrative client

Wait

Specifies whether to wait for a scheduled client operation to complete. This parameter is useful when defining client actions from a command script or macro. This parameter is optional. The default is No. Possible values are:

No
: Specifies that you do not wait for the scheduled client operation to complete. If you specify this value and the value of the ACTION parameter is COMMAND, the return code indicates whether the client action was defined.

Yes
: Specifies that you wait for the scheduled client operation to complete. If you specify this value and the value of the ACTION parameter is COMMAND, the return code indicates the status of the client operation.

You cannot issue the DEFINE CLIENTACTION command with WAIT=YES from the server console. However, from the server console, you can:

- Specify WAIT=YES with DEFINE CLIENTACTION as the command line of a DEFINE SCRIPT command.
- Specify WAIT=YES with DEFINE CLIENTACTION as the command line of a file whose contents will be read into the script that is defined by a DEFINE SCRIPT command.

Restriction: If you specify the DEFINE CLIENTACTION command with WAIT=YES in a macro, the immediate schedules defined by the command will not roll back if the macro does not complete successfully.

Example: Perform a one-time incremental backup

Issue an incremental backup command for client node TOM assigned to policy domain EMPLOYEE_RECORDS. IBM Spectrum Protect defines a schedule and associates the schedule to client node TOM (assuming that the client scheduler is running).

```
define clientaction tom domain=employee_records
action=incremental
```

Related commands

Table 1. Commands related to DEFINE CLIENTACTION

Command	Description
DELETE SCHEDULE	Deletes a schedule from the database.
QUERY ASSOCIATION	Displays the clients associated with one or more schedules.
QUERY EVENT	Displays information about scheduled and completed events for selected clients.
QUERY SCHEDULE	Displays information about schedules.
SET CLIENTACTDURATION	Specifies the duration of a schedule defined using the DEFINE CLIENTACTION command.

DEFINE CLIENTOPT (Define an option to an option set)

Use this command to add a client option to an option set.

Privilege class

To issue this command, you must have system privilege or unrestricted policy privilege.

Syntax

```
>>-DEFine CLIENTOpt--option_set_name--option_name--option_value-->

   .-Force--=--No------.
>--+-------------------+--+----------------------+-------------><
   '-Force--=--+-No--+-'  '-SEQnumber--=--number-'
               '-Yes-'
```

Parameters

option_set_name (Required)
: Specifies the name of the option set.

option_name (Required)
: Specifies a client option to add to the option set.

  See Client options that can be set by the server for a list of valid options.

  Note: To define include-exclude values, specify the include or exclude option with *option-name*, and use *option_value* to specify any valid include or exclude statement, as you would in the client options file. For example:

```
define clientopt option_set_name inclexcl "include c:\proj\text\devel.*"
```

option_value (Required)
: Specifies the value for the option. If the option includes more than one value, enclose the value in quotation marks.
Note:

1. The QUIET and VERBOSE options do not have an option value in the client option's file. To specify these values in a server client option set, specify a value of YES or NO.
2. To add an INCLUDE or EXCLUDE option for a file name that contains one or more spaces, put single quotation marks around the file specification, and double quotation marks around the entire option. See Example: Add an option to a client option set for more information.
3. The *option_value* is limited to 1024 characters.

Force
: Specifies whether the server forces the client to use the option set value. The value is ignored for additive options, such as INCLEXCL and DOMAIN. The default is NO. This parameter is optional. The values are:

  Yes
  : Specifies that the server forces the client to use the value. (The client cannot override the value.)

  No
  : Specifies that the server does not force the client to use the value. (The client can override the value.)

SEQnumber
: Specifies a sequence number when an option name is specified more than once. This parameter is optional.

Example: Add an option to a client option set

Add a client option (MAXCMDRETRIES 5) to a client option set named ENG.

```
define clientopt eng maxcmdretries 5
```

Example: Add an option to exclude a file from backup

Add a client option to the option set ENGBACKUP to exclude the c:\admin\file.txt from backup services.

```
define clientopt engbackup inclexcl "exclude c:\admin\file.txt"
```

Example: Add an option to exclude a directory from backup

Add a client option to the option set WINSPEC to exclude a temporary internet directory from backup services. When you use the EXCLUDE or INCLUDE option with file names that contain spaces, put single quotation marks around the file specification, then double quotation marks around the entire option.

```
define clientopt winspec inclexcl "exclude.dir '*:\...\Temporary Internet Files'"
```

Example: Add an option to bind files in specified directories

Add client options to the option set WINSPEC to bind all files in directories C:\Data and C:\Program Files\My Apps to a management class named PRODCLASS.

```
define clientopt winspec inclexcl "include C:\Data\...\* prodclass"
define clientopt winspec inclexcl "include 'C:\Program
   Files\My Apps\...\*' prodclass"
```

Related commands

Table 1. Commands related to DEFINE CLIENTOPT

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.

Command	Description
REGISTER NODE	Defines a client node to the server and sets options for that user.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.
UPDATE NODE	Changes the attributes that are associated with a client node.

DEFINE CLOPTSET (Define a client option set name)

Use this command to define a name for a set of options you can assign to clients for archive, backup, restore, and retrieve operations.

To add options to the new set, issue the DEFINE CLIENTOPT command.

Privilege class

To issue this command, you must have system privilege or unrestricted policy privilege.

Syntax

```
>>-DEFine CLOptset--option_set_name----------------------------->

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

option_set_name (Required)
: Specifies the name of the client option set. The maximum length of the name is 64 characters.

DESCription
: Specifies a description of the client option set. The maximum length of the description is 255 characters. The description must be enclosed in quotation marks if it contains any blank characters. This parameter is optional.

Example: Define a client option set

To define a client option set named ENG issue the following command.

```
define cloptset eng
```

Related commands

Table 1. Commands related to DEFINE CLOPTSET

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.

DEFINE COLLOCGROUP (Define a collocation group)

Use this command to define a collocation group. A *collocation group* is a group of nodes or file spaces on a node whose data is collocated on a minimal number of sequential access volumes. Their data is collocated only if the storage pool definition is set to collocate by group (COLLOCATE=GROUP).

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

```
>>-DEFine COLLOCGroup--group_name------------------------------>

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

group_name
: Specifies the name of the collocation group name that you want to create. The maximum length of the name is 30 characters.

DESCription
: Specifies a description of the collocation group. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Define a collocation group

To define a node or file space collocation group named GROUP1, issue the following command:

```
define collocgroup group1
```

Related commands

Table 1. Commands related to DEFINE COLLOCGROUP

Command	Description
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

DEFINE COLLOCMEMBER (Define collocation group member)

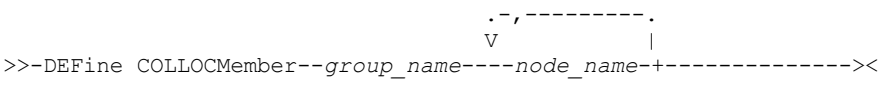
Issue this command to add a client node to a collocation group or to add a file space from a node to a collocation group. A collocation group is a group of nodes or file spaces on a node whose data is collocated on a minimal number of sequential access volumes.

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

Add a node to a collocation group

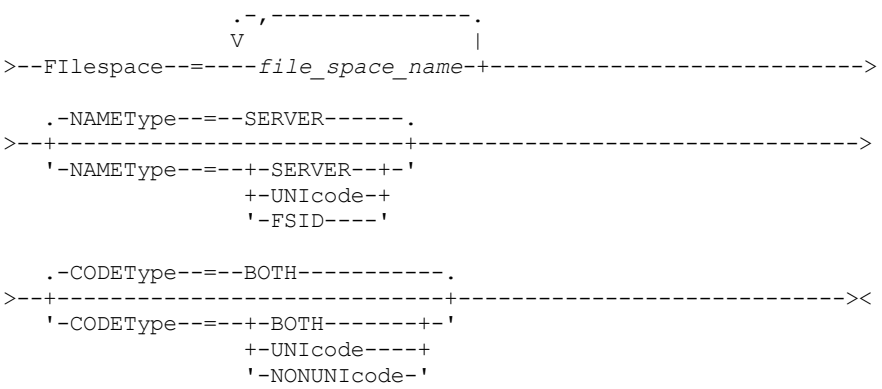


Parameters

group_name
: Specifies the name of the collocation group to which you want to add a client node.

node_name
: Specifies the name of the client node that you want to add to the collocation group. You can specify one or more names. Separate multiple names with commas; do not use intervening spaces. You can also use wildcard characters to specify multiple names.

Add a file space from a node to a collocation group



Parameters

group_name
: Specifies the name of the collocation group to which you want to add a file space.

node_name
: Specifies the client node where the file space is located.

FIlespace
: Specifies the *file_space_name* on the client node that you want to add to the collocation group. You can specify one or more file space names that are on a specific client node. If you specify multiple file space names, separate the names with commas with no intervening spaces. You can also use wildcard characters to specify multiple file space names. For example:

```
define collocmember manufacturing linux237 filespace=*_linux_fs
```

This command places all file spaces on the linux237 node with a name that ends with _linux_fs into the manufacturing collocation group.
See the following list for tips about working with collocation groups:

- When you add members to a new collocation group, the type of the first collocation group member determines the type of the collocation group. The group can either be a node collocation group or a file space collocation group. Restriction: After the collocation group type is set, it cannot be changed.
- You cannot mix collocation group member types when you add members to a collocation group (either a node group or a file space group).
- For a file space collocation group, you can add file spaces to the group. The file spaces must use the same value as the *node_name* parameter that is specified when the collocation group is established.
- A client node can be included in multiple file space groups. However, if a node is a member of a node collocation group, it cannot be a member of a file space collocation group.
- A file space can be a member of only one file space group.

NAMEType
: Specify how you want the server to interpret the file space names that you enter. Specify this parameter when the server communicates with clients that have Unicode support. A backup-archive client with Unicode support is available only for Windows, Macintosh OS 9, Macintosh OS X, and NetWare systems. The filespace name cannot be a wildcard character when NAMETYPE is specified for a filespace collocation group. The default value is SERVER. You can specify one of the following values:

  SERVER
  : The server uses the server code page to interpret the file space names.

  UNIcode
  : The server converts the file space names from the server code page to the UTF-8 code page. Whether the name can be converted depends on the characters in the names and the server code page. Conversion might fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

  FSID
  : The server interprets the file space names by their file space IDs (FSIDs).

CODEType
: Specify how you want the server to interpret the file space names that you enter. Use this parameter when you use a wildcard character for the file space name. For example:

  ```
  define collocmember production Win_3419 filespace=* codetype=unicode
  ```

  This example command adds all file spaces from the Win_3419 node to the production collocation group. The default is BOTH, so the file spaces are included, regardless of code page type. You can specify one of the following values:

  BOTH
  : Include the file spaces, regardless of code page type.

  UNIcode
  : Include file spaces that are only in Unicode.

  NONUNIcode
  : Include file spaces that are not in Unicode.

Define two collocation group members

Define two members, NODE1 and NODE2, to a collocation group, GROUP1.

```
define collocmember group1 node1,node2
```

Define one file space group member CNTR90524, on node clifton to collocation group TSM_alpha_1

```
define collocmember TSM_alpha_1 clifton filespace=CNTR90524
```

Related commands

Table 1. Commands related to DEFINE COLLOCMEMBER

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

DEFINE COPYGROUP (Define a copy group)

Use this command to define a new backup or archive copy group within a specific management class, policy set, and policy domain. The server uses the backup and archive copy groups to control how clients back up and archive files, and to manage the backed-up and archived files.

To enable clients to use the new copy group, you must activate the policy set that contains the new copy group.

You can define one backup and one archive copy group for each management class. To ensure that client nodes can back up files, include a backup copy group in the default management class for a policy set.

Attention: The DEFINE COPYGROUP command fails if you specify a copy storage pool as a destination.

The DEFINE COPYGROUP command has two forms, one for defining a backup copy group and one for defining an archive copy group. The syntax and parameters for each form are defined separately.

Table 1. Commands related to DEFINE COPYGROUP

Command	Description
ASSIGN DEFMGMTCLASS	Assigns a management class as the default for a specified policy set.
BACKUP NODE	Backs up a network-attached storage (NAS) node.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE MGMTCLASS	Defines a management class.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COPYGROUP	Deletes a backup or archive copy group from a policy domain and policy set.

Command	Description
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
EXPIRE INVENTORY	Manually starts inventory expiration processing.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.
SET ARCHIVERETENTIONPROTECTION	Specifies whether data retention protection is activated.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

- DEFINE COPYGROUP (Define a backup copy group)
  Use this command to define a new backup copy group within a specific management class, policy set, and policy domain.
- DEFINE COPYGROUP (Define an archive copy group)
  Use this command to define a new archive copy group within a specific management class, policy set, and policy domain.

DEFINE COPYGROUP (Define a backup copy group)

Use this command to define a new backup copy group within a specific management class, policy set, and policy domain.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the copy group belongs.

Syntax

```
>>-DEFine COpygroup--domain_name--policy_set_name--class_name--->

   .-STANDARD-.  .-Type--=--Backup-.
>--+----------+--+-----------------+---------------------------->
   '-STANDARD-'  '-Type--=--Backup-'

                              .-FREQuency--=--0----.
>--DESTination--=--pool_name--+-------------------+------------>
                              '-FREQuency--=--days-'

   .-VERExists--=--2-----------.
>--+---------------------------+------------------------------->
   '-VERExists--=--+-number--+-'
                   '-NOLimit-'

   .-VERDeleted--=--1-----------.
>--+----------------------------+------------------------------>
   '-VERDeleted--=--+-number--+-'
                    '-NOLimit-'

   .-RETExtra--=--30----------.  .-RETOnly--=--60----------.
>--+-------------------------+--+-------------------------+---->
   '-RETExtra--=--+-days----+-'  '-RETOnly--=--+-days----+-'
                  '-NOLimit-'                  '-NOLimit-'

   .-MODE--=--MODified-----.
>--+----------------------+----------------------------------->
   '-MODE--=--+-MODified-+-'
              '-ABSolute-'

   .-SERialization--=--SHRSTatic------.
>--+--------------------------------+------------------------->
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'

>--+--------------------------------+------------------------><
```

```
'-TOCDestination--=----pool_name---'
```

Parameters

domain_name (Required)
: Specifies the policy domain for which you are defining the copy group.

policy_set_name (Required)
: Specifies the policy set for which you are defining the copy group.

  You cannot define a copy group for a management class that belongs to the ACTIVE policy set.

class_name (Required)
: Specifies the management class for which you are defining the copy group.

STANDARD
: Specifies the name of the copy group, which must be STANDARD. This parameter is optional. The default value is STANDARD.

Type=Backup
: Specifies that you want to define a backup copy group. The default parameter is BACKUP. This parameter is optional.

DESTination (Required)
: Specifies the primary storage pool where the server initially stores backup data. You cannot specify a copy storage pool as the destination.

FREQuency
: Specifies how frequently IBM Spectrum Protect™ can back up a file. This parameter is optional. IBM Spectrum Protect backs up a file only when the specified number of days has elapsed since the last backup. The FREQUENCY value is used only during a full incremental backup operation. This value is ignored during selective backup or partial incremental backup. You can specify an integer from 0 to 9999. The default value is 0, meaning that IBM Spectrum Protect can back up a file regardless of when the file was last backed up.

VERExists
: Specifies the maximum number of backup versions to retain for files that are currently on the client file system. This parameter is optional. The default value is 2.
  If an incremental backup operation causes the limit to be exceeded, the server expires the oldest backup version that exists in server storage. Possible values are:

  number
  : Specifies the number of backup versions to retain for files that are currently on the client file system. You can specify an integer from 1 to 9999.
    Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 2. Preferred values are 3, 4, or more.

  NOLimit
  : Specifies that you want the server to retain all backup versions.

  The number of backup versions to retain is controlled by this parameter until versions exceed the retention time specified by the RETEXTRA parameter.

VERDeleted
: Specifies the maximum number of backup versions to retain for files that have been deleted from the client file system after being backed up using IBM Spectrum Protect. This parameter is optional. The default value is 1.
  If a user deletes a file from the client file system, the next incremental backup causes the server to expire the oldest versions of the file in excess of this number. The expiration date for the remaining versions is determined by the retention time specified by the RETEXTRA or RETONLY parameter. Possible values are:

  number
  : Specifies the number of backup versions to retain for files that are deleted from the client file system after being backed up. You can specify an integer from 0 to 9999.

  NOLimit
  : Specifies that you want the server to retain all backup versions for files that are deleted from the client file system after being backed up.

RETExtra
: Specifies the number of days to retain a backup version after that version becomes inactive. A version of a file becomes inactive when the client stores a more recent backup version, or when the client deletes the file from the workstation and then runs a full incremental backup. The server deletes inactive versions based on retention time even if the number of

inactive versions does not exceed the number allowed by the VEREXISTS or VERDELETED parameters. This parameter is optional. The default value is 30 days. Possible values are:

days
Specifies the number of days to retain inactive backup versions. You can specify an integer from 0 to 9999.
Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 14 days. The preferred value is 30 or more days.

NOLimit
Specifies that you want to retain inactive backup versions indefinitely.

If you specify NOLIMIT, the server deletes inactive backup versions based on the VEREXISTS parameter (when the file still exists on the client file system) VERDELETED parameter (when the file no longer exists on the client file system).

RETOnly
Specifies the number of days to retain the last backup version of a file that has been deleted from the client file system. This parameter is optional. The default value is 60. Possible values are:

days
Specifies the number of days to retain the last remaining inactive version of a file. You can specify an integer from 0 to 9999.
Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 30 days.

NOLimit
Specifies that you want to keep the last remaining inactive version of a file indefinitely.

If you specify NOLIMIT, the server retains the last remaining backup version forever, unless a user or administrator deletes the file from server storage.

MODE
Specifies whether IBM Spectrum Protect backs up a file only if the file has changed since the last backup, or whenever a client requests a backup. This parameter is optional. The default value is MODIFIED. Possible values are:

MODified
Specifies that IBM Spectrum Protect backs up the file only if it has changed since the last backup. IBM Spectrum Protect considers a file changed if any of the following is true:

- The date last modified is different
- The file size is different
- The file owner is different
- The file permissions are different

ABSolute
Specifies that IBM Spectrum Protect backs up the file regardless of whether it has been modified.

The MODE value is used only for full incremental backup. This value is ignored during partial incremental backup or selective backup.

SERialization
Specifies how IBM Spectrum Protect processes files or directories when they are modified during backup processing. This parameter is optional. The default value is SHRSTATIC. Possible values are:

SHRSTatic
Specifies that IBM Spectrum Protect backs up a file or directory only if it is not being modified during backup. IBM Spectrum Protect attempts to perform a backup as many as four times, depending on the value specified for the CHANGINGRETRIES client option. If the file or directory is modified during each backup attempt, IBM Spectrum Protect does not back it up.

STatic
Specifies that IBM Spectrum Protect backs up a file or directory only if it is not being modified during backup. IBM Spectrum Protect attempts to perform the backup only once.

Platforms that do not support the STATIC option default to SHRSTATIC.

SHRDYnamic

Specifies that if the file or directory is being modified during a backup attempt, IBM Spectrum Protect backs up the file or directory during the last attempt even though the file or directory is being modified. IBM Spectrum Protect attempts to perform a backup as many as four times, depending on the value specified for the CHANGINGRETRIES client option.

DYnamic

Specifies that IBM Spectrum Protect backs up a file or directory on the first attempt, regardless of whether the file or directory is being modified during backup processing.

Attention: Be careful about using the SHRDYNAMIC and DYNAMIC values. IBM Spectrum Protect uses these values to determine if it backs up a file or directory while modifications are occurring. As a result, the backup version might be a fuzzy backup. A fuzzy backup does not accurately reflect what is currently in the file or directory because it contains some, but not all, modifications. If a file that contains a fuzzy backup is restored, the file may or may not be usable, depending on the application that uses the file. If a fuzzy backup is not acceptable, set SERIALIZATION to SHRSTATIC or STATIC so that IBM Spectrum Protect creates a backup version only if the file or directory is not being modified.

TOCDestination

Specifies the primary storage pool in which a table of contents (TOC) will initially be stored for any Network Data Management Protocol (NDMP) backup or backup set operation for which a TOC is generated. This parameter is optional. You cannot specify a copy storage pool as the destination. The storage pool specified for the destination must have NATIVE or NONBLOCK data format. To avoid mount delays, it is recommended that the storage pool have a device class of DISK or DEVTYPE=FILE. TOC generation is an option for NDMP backup operations, but is not supported for other image-backup operations.

If TOC creation is requested for a backup operation that uses NDMP and the image is bound to a management class whose backup copy group does not specify a TOC destination, the outcome will depend on the TOC parameter for the backup operation.

- If TOC=PREFERRED (the default), the backup proceeds without creation of a TOC.
- If TOC=YES, the entire backup fails because no TOC can be created.

Example: Create a backup copy group

Create a backup copy group named STANDARD for management class ACTIVEFILES in policy set VACATION in the EMPLOYEE_RECORDS policy domain. Set the backup destination to BACKUPPOOL. Set the minimum interval between backups to three days, regardless of whether the files have been modified. Retain up to five backup versions of a file while the file exists on the client file system.

```
define copygroup employee_records
vacation activefiles standard type=backup
destination=backuppool frequency=3
verexists=5 mode=absolute
```

DEFINE COPYGROUP (Define an archive copy group)

Use this command to define a new archive copy group within a specific management class, policy set, and policy domain.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the copy group belongs.

Syntax

```
>>-DEFine COpygroup--domain_name--policy_set_name--class_name--->

   .-STANDARD-.
>--+----------+--Type--=--Archive--DESTination--=--pool_name---->
   '-STANDARD-'

   .-FREQuency--=--Cmd-.  .-RETVer--=--365---------.
>--+-------------------+--+-----------------------+------------>
   '-FREQuency--=--Cmd-'  '-RETVer--=--+-days----+-'
                                       '-NOLimit-'
```

```
   .-RETInit--=--CREATion--.  .-RETMin--=--365------.
>--+----------------------+--+--------------------+----------->
   '-RETInit--=-----EVent---'  '-RETMin--=-----days---'

   .-MODE--=--ABSolute-.
>--+-------------------+---------------------------------------->
   '-MODE--=--ABSolute-'

   .-SERialization--=--SHRSTatic------.
>--+--------------------------------+----------------------><
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain for which you are defining the copy group.

policy_set_name (Required)
: Specifies the name of the policy set for which you are defining the copy group.

  You cannot define a copy group for a management class that belongs to the ACTIVE policy set.

class_name (Required)
: Specifies the name of the management class for which you are defining the copy group.

STANDARD
: Specifies the name of the copy group, which must be STANDARD. This parameter is optional. The default value is STANDARD.

Type=Archive (Required)
: Specifies that you want to define an archive copy group.

DESTination (Required)
: Specifies the primary storage pool where the server initially stores the archive copy. You cannot specify a copy storage pool as the destination.

FREQuency=Cmd
: Specifies the copy frequency, which must be CMD. This parameter is optional. The default value is CMD.

RETVer
: Specifies the number of days to keep an archive copy. This parameter is optional. The default value is 365. Possible values are:

  days
  : Specifies the length of time to keep an archive copy. You can specify an integer in the range 0 - 30000.
    Tip: To help ensure that your data can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 30 days.
    The RETENTIONEXTENSION server option can affect the volume retention if the following conditions are true:

    - You specify zero for the number of days
    - The destination storage pool for the archive copy group is a SnapLock storage pool (RECLAMATIONTYPE=SNAPLOCK)

    If the two conditions are met, retention of the volumes is defined by the value of the RETENTIONEXTENSION server option. The RETENTIONEXTENSION server option value also applies if data is copied or moved into the SnapLock storage pool by a server process such as migration, or by using the MOVE DATA or MOVE NODEDATA commands.

  NOLimit
  : Specifies that you want to keep an archive copy indefinitely.

    If you specify NOLIMIT, the server retains archive copies forever, unless a user or administrator deletes the file from server storage. If you specify NOLIMIT, you cannot also specify EVENT for the RETINIT parameter.

  The value of the RETVER parameter can affect the management class to which the server binds an archived directory. If the client does not use the ARCHMC option, the server binds directories that are archived to the default management class. If the default management class has no archive copy group, the server binds directories that are archived to the management class with the shortest retention period.

The RETVER parameter of the archive copy group of the management class to which an object is bound determines the retention criterion for each object. See the SET ARCHIVERETENTIONPROTECTION command for a description of data protection.

If the primary storage pool specified in the DESTINATION parameter belongs to a Centera device class and data protection is enabled, then the RETVER value is sent to Centera for retention management purposes. See the SET ARCHIVERETENTIONPROTECTION command for a description of data protection.

RETInit
: Specifies when the retention time specified by the RETVER attribute is initiated. This parameter is optional. If you define the RETINIT value during copy group creation, you cannot modify it later. The default value is CREATION. Possible values are:

  CREATion
  : Specifies that the retention time specified by the RETVER attribute is initiated at the time an archive copy is stored on the IBM Spectrum Protect™ server.

  EVent
  : Specifies that the retention time specified in the RETVER parameter is initiated at the time a client application notifies the server of a retention-initiating event for the archive copy. If you specify RETINIT=EVENT, you cannot also specify RETVER=NOLIMIT.

  Tip: You can place a deletion hold on an object that was stored with RETINIT=EVENT for which the event has not been signaled. If the event is signaled while the deletion hold is in effect, the retention period is initiated, but the object is not deleted while the hold is in effect.

RETMin
: Specifies the minimum number of days to keep an archive copy after it is archived. This parameter is optional. The default value is 365. If you specify RETINIT=CREATION, this parameter is ignored.

MODE=ABSolute
: Specifies that a file is always archived when the client requests it. The MODE must be ABSOLUTE. This parameter is optional. The default value is ABSOLUTE.

SERialization
: Specifies how IBM Spectrum Protect processes files that are modified during archive. This parameter is optional. The default value is SHRSTATIC. Possible values are:

  SHRSTatic
  : Specifies that IBM Spectrum Protect archives a file only if it is not being modified. IBM Spectrum Protect attempts to perform an archive operation as many as four times, depending on the value that is specified for the CHANGINGRETRIES client option. If the file is modified during the archive attempt, IBM Spectrum Protect does not archive the file.

  STatic
  : Specifies that IBM Spectrum Protect archives a file only if it is not being modified. IBM Spectrum Protect attempts to perform the archive operation only once.

    Platforms that do not support the STATIC option default to SHRSTATIC.

  SHRDYnamic
  : Specifies that if the file is being modified during an archive attempt, IBM Spectrum Protect archives the file during its last attempt even though the file is being modified. IBM Spectrum Protect attempts to archive the file as many as four times, depending on the value that is specified for the CHANGINGRETRIES client option.

  DYnamic
  : Specifies that IBM Spectrum Protect archives a file on the first attempt, regardless of whether the file is being modified during archive processing.
    Attention: Be careful about using the SHRDYNAMIC and DYNAMIC values. IBM Spectrum Protect uses them to determine if it archives a file while modifications are occurring. As a result, the archive copy might be a fuzzy backup. A fuzzy backup does not accurately reflect what is in the file because it contains some, but not all, modifications. If a file that contains a fuzzy backup is retrieved, the file might or might not be usable, depending on the application that uses the file. If a fuzzy backup is not acceptable, set SERIALIZATION to SHRSTATIC or STATIC so that IBM Spectrum Protect creates an archive copy only if the file is not being modified.

Example: Define an archive copy group for event-based retention

Create an archive copy group named STANDARD for management class EVENTMC in policy set SUMMER in the PROG1 policy domain. Set the archive destination to ARCHIVEPOOL, where the archive copy is kept until the server is notified of an event to

initiate the retention time, after which the archive copy is kept for 30 days. The archive copy will be kept for a minimum of 90 days after being stored on the server, regardless of when the server is notified of an event to initiate the retention time.

```
define copygroup prog1 summer eventmc standard type=archive
destination=archivepool retinit=event retver=30 retmin=90
```

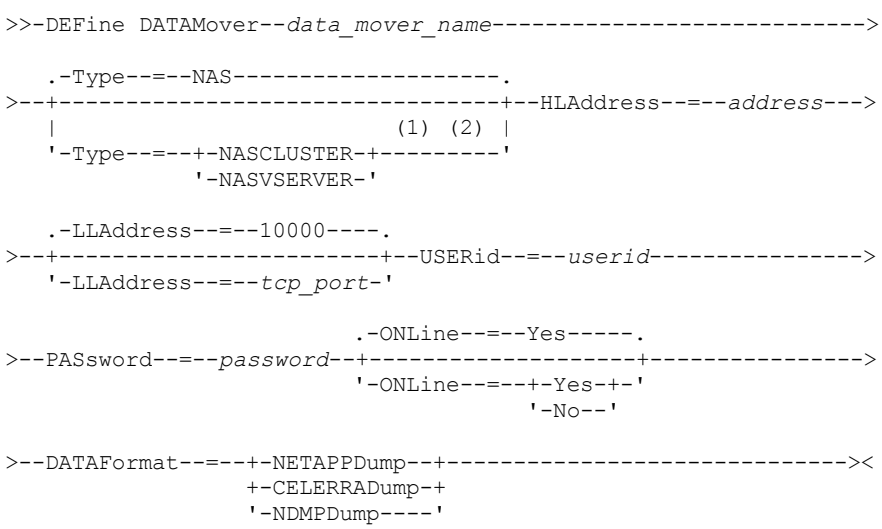
DEFINE DATAMOVER (Define a data mover)

Use this command to define a data mover. A data mover is a named device that accepts a request from IBM Spectrum Protect™ to transfer data. A data mover can be used to complete outboard copy operations.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Notes:

1. You can specify `TYPE=NASCLUSTER` and `TYPE=NASVSERVER` only on an AIX®, Linux, or Windows operating system.
2. You can specify `TYPE=NASCLUSTER` and `TYPE=NASVSERVER` only if `DATAFORMAT=NETAPPDUMP`.

Parameters

data_mover_name (Required)
: Specifies the name of the data mover. This name must be the same as a node name that you previously registered by using the `REGISTER NODE TYPE=NAS` command. The data that is backed up from this NAS data mover will be assigned to this node name in the server database. A maximum of 64 characters can be used to specify the name.

Type
: Specifies the type of data mover. This parameter is optional. The default value is NAS.

  NAS
  : Specifies that the data mover is a NAS file server.

  NASCLUSTER
  : Specifies that the data mover is a clustered NAS file server.
  Restriction: You can specify the NASCLUSTER value only if `DATAFORMAT=NETAPPDUMP`.

  NASVSERVER
  : Specifies that the data mover is a virtual storage device within a cluster.
  Restriction: You can specify the NASVSERVER value only if `DATAFORMAT=NETAPPDUMP`.

HLAddress (Required)
: Specifies either the numerical IP address or the domain name that is used to access the NAS file server.

Tip: To determine the numerical IP address, access the NAS file server. Then, follow the instructions in the file server documentation for obtaining the address.

LLAddress
Specifies the TCP port number to access the NAS device for Network Data Management Protocol (NDMP) sessions. This parameter is optional. The default value is 10000.

USERid (Required)
Specifies the user ID for a user that is authorized to initiate an NDMP session with the NAS file server. For example, enter the user ID that is configured on the NetApp file server for NDMP connections.
Tip: To determine the user ID, access the NAS file server. Then, follow the instructions in the file server documentation for obtaining the user ID.

PASsword (Required)
Specifies the password for the user ID to log on to the NAS file server.
Tip: To determine the password, access the NAS file server. Then, follow the instructions in the file server documentation for obtaining the password.

ONLine
Specifies whether the data mover is available for use. This parameter is optional. The default is YES.

Yes
The default value. Specifies that the data mover is available for use.

No
Specifies that the data mover is not available for use. When the hardware is being maintained, you can use the UPDATE DATAMOVER command to set the data mover offline.

If a library is controlled by using a path from a NAS data mover to the library, and the NAS data mover is offline, the server is not able to access the library. If the server is halted and restarted while the NAS data mover is offline, the library is not initialized.

DATAFormat (Required)
Specifies the data format that is used by this data mover.

NETAPPDump
Must be used for NetApp NAS file servers and the IBM® System Storage® N Series.

CELERRADump
Must be used for EMC Celerra NAS file servers.

NDMPDump
Must be used for NAS file servers other than NetApp or EMC file servers.

Example: Define a data mover by domain name

Define a data mover for the node named NAS1. The domain name for the data mover is NETAPP2.EXAMPLE.COM at port 10000.

```
define datamover nas1 type=nas hladdress=netapp2.example.com lladdress=10000
    userid=root password=admin dataformat=netappdump
```

Example: Define a data mover by IP address

Define a data mover for the node named NAS2. The numerical IP address for the data mover is 203.0.113.0, at port 10000. The NAS file server is not a NetApp or EMC file server.

```
define datamover nas2 type=nas hladdress=203.0.113.0 lladdress=10000
    userid=root password=admin dataformat=ndmpdump
```

Example: Define a data mover for a clustered file server by IP address

Define a data mover for the clustered file server named NAS3. The NAS file server is a NetApp device. The numerical IP address for the data mover is 198.51.100.0, at port 10000.

```
define datamover nas3 type=nascluster hladdress=198.51.100.0
    lladdress=10000 userid=root password=admin dataformat=netappdump
```

Related commands

Table 1. Commands related to DEFINE DATAMOVER

Command	Description
DEFINE PATH	Defines a path from a source to a destination.
DELETE DATAMOVER	Deletes a data mover.
QUERY DATAMOVER	Displays data mover definitions.
REGISTER NODE	Defines a client node to the server and sets options for that user.
UPDATE DATAMOVER	Changes the definition for a data mover.

DEFINE DEVCLASS (Define a device class)

Use this command to define a device class for a type of storage device. The server requires that a device class be defined to allow the use of a device.

For the most up-to-date list of supported devices and valid device class formats, see the IBM Spectrum Protect™ Supported Devices website: AIX Windows

- Supported devices for AIX and Windows

Linux

- Supported devices for Linux

Note: The DISK device class is defined by IBM Spectrum Protect and cannot be modified with the DEFINE DEVCLASS command.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see Define device class for z/OS media server.

The following IBM Spectrum Protect device classes are ordered by device type.

- r_cmd_devclass_3590_define.dita#r_cmd_devclass_3590_define
- r_cmd_devclass_3592_define.dita#r_cmd_devclass_3592_define
- r_cmd_devclass_4mm_define.dita#r_cmd_devclass_4mm_define
- r_cmd_devclass_8mm_define.dita#r_cmd_devclass_8mm_define
- r_cmd_devclass_centera_define.dita#r_cmd_devclass_centera_define
- r_cmd_devclass_dlt_define.dita#r_cmd_devclass_dlt_define
- r_cmd_devclass_ecartridge_define.dita#r_cmd_devclass_ecartridge_define
- r_cmd_devclass_file_define.dita#r_cmd_devclass_file_define
- AIX Windows r_cmd_devclass_generictape_define.dita#r_cmd_devclass_generictape_define
- r_cmd_devclass_lto_define.dita#r_cmd_devclass_lto_define
- r_cmd_devclass_nas_define.dita#r_cmd_devclass_nas_define
- r_cmd_devclass_removablefile_define.dita#r_cmd_devclass_removablefile_define
- r_cmd_devclass_server_define.dita#r_cmd_devclass_server_define
- r_cmd_devclass_volsafe_define.dita#r_cmd_devclass_volsafe_define

Table 1. Commands related to DEFINE DEVCLASS

Command	Description
BACKUP DEVCONFIG	Backs up IBM Spectrum Protect device information to a file.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE DEVCLASS	Deletes a device class.
QUERY DEVCLASS	Displays information about device classes.
QUERY DIRSPACE	Displays information about FILE directories.
UPDATE DEVCLASS	Changes the attributes of a device class.

DEFINE DEVCLASS (Define a 3590 device class)

Use the 3590 device class when you are using 3590 tape devices.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see DEFINE DEVCLASS (Define a 3590 device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--------------------------->

>--LIBRary--=--library_name--DEVType--=--3590------------------->

   .-FORMAT--=--DRIVE-------.
>--+-----------------------+--+---------------------+--------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--size-'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
                +-3590E-C-+
                +-3590H-B-+
                '-3590H-C-'

   .-PREFIX--=--ADSM-------------------.
>--+---------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+--------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

: Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

: For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=3590 (Required)
: Specifies the 3590 device type is assigned to the device class. 3590 indicates that IBM® 3590 cartridge tape devices are assigned to this device class.

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

: If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other

must have LTO-6 drives and media.

The following tables list the recording formats, estimated capacities, and recording format options for 3590 devices:

Table 1. Recording formats and default estimated capacities for 3590

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
3590B	10.0 GB	Uncompressed (basic) format
3590C	See note 20.0 GB	Compressed format
3590E-B	10.0 GB	Uncompressed (basic) format, similar to the 3590B format
3590E-C	See note 20.0 GB	Compressed format, similar to the 3590C format
3590H-B	30.0 GB (J cartridge – standard— length) 60.0 GB (K cartridge - extended length)	Uncompressed (basic) format, similar to the 3590B format
3590H-C	See note 60.0 GB (J cartridge - standard length) 120.0 GB (K cartridge - extended length)	Compressed format, similar to the 3590C format
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be greater than the listed value.		

Table 2. 3590 device recording format selections

Device	Format					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Read/Write	Read/Write	–	–	–	–
Ultra SCSI	Read/Write	Read/Write	–	–	–	–
3590E	Read	Read	Read/Write	Read/Write	–	–
3590H	Read	Read	Read	Read	Read/Write	Read/Write

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

```
AB.CD2.E
```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DEFINE DEVCLASS (Define a 3592 device class)

Use the 3592 device class when you are using 3592 tape devices.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see DEFINE DEVCLASS (Define a 3592 device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name-------------------------->

>--LIBRary--=--library_name--DEVType--=--3592------------------>

                                                    (1)
   .-LBProtect--=--No------------.  .-WORM--=--No------.
>--+-----------------------------+--+------------------+-------->
   '-LBProtect--=--+-READWrite-+-'  '-WORM--=--+-Yes-+-'
                   +-WRITEOnly-+               '-No--'
                   '-No--------'

   .-SCALECAPacity--=--100-----.  .-FORMAT--=--DRIVE--------.
>--+---------------------------+--+-------------------------+--->
   '-SCALECAPacity--=--+-100-+-'  '-FORMAT--=--+-DRIVE----+-'
                       +-90--+                 +-3592-----+
                       '-20--'                 +-3592C----+
                                               +-3592-2---+
                                               +-3592-2C--+
                                               +-3592-3---+
                                               +-3592-3C--+
                                               +-3592-4---+
                                               +-3592-4C--+
                                               +-3592-5---+
                                               +-3592-5C--+
                                               +-3592-5A--+
                                               '-3592-5AC-'

>--+---------------------+----------------------------------->
   '-ESTCAPacity--=--size-'

   .-PREFIX--=--ADSM-------------------.
>--+--------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'

                               (1)  (2)
   .-DRIVEEncryption--=--ALLOW---------.
>--+---------------------------------+----------------------><
   '-DRIVEEncryption--=--+-ON-------+--'
                         +-ALLOW----+
                         +-EXTERNAL-+
                         '-OFF------'
```

Notes:

1. You cannot specify both WORM=Yes and DRIVEENCRYPTION=ON.
2. Drive encryption is supported only for 3592 Generation 2 or later drives.

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=3592 (Required)
Specifies that the 3592 device type is assigned to the device class.

LBProtect

Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

The default is NO.

The following values are possible:

READWrite
Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect™ and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

WRITEOnly
Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

No
Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

Restriction: Logical block protection is supported only on IBM® 3592 Generation 3 drives and later with 3592 Generation 2 media and later.

See Technote 1634851, Additional information on the IBM Spectrum Protect LBProtect option, for an explanation about when to use the LBProtect parameter.

WORM
Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. The field can contain one of the following values:

Yes
Specifies that the drives use WORM media.

No
Specifies that the drives do not use WORM media.

Remember:

1. To use 3592 WORM support in 3584 libraries, you must specify the WORM parameter. The server distinguishes between WORM and non-WORM scratch volumes. However, to use 3592 WORM support in 349X libraries, you also must set the WORMSCRATCHCATEGORY on the DEFINE LIBRARY command. For details, see DEFINE LIBRARY (Define a library).
2. When WORM=Yes, the only valid value for the SCALECAPACITY parameter is 100.
3. Verify with your hardware vendors that your hardware is at the appropriate level of support.

SCALECAPacity
Specifies the percentage of the media capacity that can be used to store data. This parameter is optional. The default is 100. Possible values are 20, 90, or 100.

Setting the scale capacity percentage to 100 provides maximum storage capacity. Setting it to 20 provides fastest access time.

Note: The scale capacity value takes effect only when data is first written to a volume. Any updates to the device class for scale capacity do not affect volumes that already have data that is written to them until the volume is returned to scratch status.

FORMAT

Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats, estimated capacities, and recording format options for 3592 devices.
Tip: The format name is specified as, for example, 3592-X, 3592-XC, 3592-XA, or 3592-XAC, where X indicates the drive generation, C indicates a compressed format, and A indicates an archive drive.

Table 1. Recording formats and default estimated capacities for 3592

Format	Estimated capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
3592	300 GB	Uncompressed (basic) format
3592C	See note.	Compressed format
3592-2	500 GB 700 GB	Uncompressed (basic) format JA tapes Uncompressed (basic) format JB tapes
3592-2C	1.5 TB 2.1 TB	Compressed format JA tapes Compressed format JB tapes
3592–3	640 GB 1 TB	Uncompressed (basic) format JA tapes Uncompressed (basic) format JB tapes
3592–3C	1.9 TB 3 TB	Compressed format JA tapes Compressed format JB tapes
3592-4	400 GB 1.5 TB 3.1 TB	Uncompressed (basic) format JK tapes Uncompressed (basic) format JB tapes Uncompressed (basic) format JC tapes
3592-4C	1.2 TB 4.4 TB 9.4 TB	Compressed format JK tapes Compressed format JB tapes Compressed format JC tapes

Format	Estimated capacity	Description
3592-5 (For IBM TS1150 Model 3592 E08 drives with product ID 03592E08)	900 GB 7 TB 2 TB 10 TB	Uncompressed (basic) format JK tapes Uncompressed (basic) format JC/JY tapes Uncompressed (basic) format JL tapes Uncompressed (basic) format JD/JZ tapes
3592-5C (For IBM TS1150 Model 3592 E08 drives with product ID 03592E08)	Depends on the compressibility of the data	Compressed format JK tapes Compressed format JC/JY tapes Compressed format JL tapes Compressed format JD/JZ tapes
3592-5A (For IBM TS1155 Model 3592 55F drives with product ID 0359255F)	3 TB 15 TB	Uncompressed (basic) format JL tapes Uncompressed (basic) format JD/JZ tapes
3592-5AC (For IBM TS1155 Model 3592 55F drives with product ID 0359255F)	Depends on the compressibility of the data	Compressed format JL tapes Compressed format JD/JZ tapes
Note: If this format uses the compression feature for tape drives, depending on the effectiveness of compression, the actual capacity might be different from the estimated capacity.		

Important: For optimal performance, avoid mixing different generations of drives in a single SCSI library. If you must mix drive generations in a SCSI library, use one of the special configurations that are described in the topic about mixing generations of 3592 media.

Special configurations are also required for mixing different generations of 3592 drives in 349x and ACSLS libraries.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption
Specifies whether drive encryption is allowed. This parameter is optional. The default is ALLOW.

ON
Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes-for example, back up sets, export volumes, and database backup volumes-will not be encrypted.) If you specify ON and you enable either the library or system method of encryption, drive encryption is not allowed and backup operations fail.

ALLOW
Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if either the library or system method of encryption is enabled.

EXTERNAL
Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive.
When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption.

By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF

Specifies that drive encryption is not allowed. If you enable either the library or system method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

DEFINE DEVCLASS (Define a 4MM device class)

Use the 4MM device class when you are using 4 mm tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name-------------------------->

>--LIBRary--=--library_name--DEVType--=--4MM-------------------->

   .-FORMAT--=--DRIVE-----.
>--+----------------------+--+----------------------+---------->
   '-FORMAT--=--+-DRIVE-+-'  '-ESTCAPacity--=--size-'
                +-DDS1--+
                +-DDS1C-+
                +-DDS2--+
                +-DDS2C-+
                +-DDS3--+
                +-DDS3C-+
                +-DDS4--+
                +-DDS4C-+
                +-DDS5--+
                +-DDS5C-+
                +-DDS6--+
                '-DDS6C-'

   .-PREFIX--=--ADSM-------------------.
>--+-----------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTWait--=--60------.  .-MOUNTRetention--=--60------.
>--+----------------------+--+---------------------------+---->
   '-MOUNTWait--=--minutes-'  '-MOUNTRetention--=--minutes-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)

Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

Specifies the name of the defined library object that contains the 4 mm tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=4MM (Required)

Specifies that the 4MM device type is assigned to the device class. The 4MM indicates that 4 mm tape devices are assigned to this device class.

FORMAT

Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for 4 mm devices:

Table 1. Recording formats and default estimated capacities for 4 mm tapes

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
DDS1	2.6 GB (60 meter) 4.0 GB (90 meter)	Uncompressed format, applies only to 60-meter and 90-meter tapes
DDS1C	See note 1.3 GB (60 meter) 2.0 GB (90 meter)	Compressed format, applies only to 60-meter and 90-meter tapes
DDS2	4.0 GB	Uncompressed format, applies only to 120-meter tapes
DDS2C	See note 8.0 GB	Compressed format, applies only to 120-meter tapes
DDS3	12.0 GB	Uncompressed format, applies only to 125-meter tapes
DDS3C	See note 24.0 GB	Compressed format, applies only to 125-meter tapes
DDS4	20.0 GB	Uncompressed format, applies only to 150-meter tapes
DDS4C	See note 40.0 GB	Compressed format, applies only to 150-meter tapes
DDS5	36 GB	Uncompressed format, when using DAT 72 media
DDS5C	See note 72 GB	Compressed format, when using DAT 72 media
DDS6	80 GB	Uncompressed format, when using DAT 160 media
DDS6C	See note 160 GB	Compressed format, when using DAT 160 media
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be greater than the listed value.		

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

For more information about the default estimated capacity for 4 mm tapes, see Table 1

PREFIX

Specifies the high-level qualifier of the file name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DEFINE DEVCLASS (Define an 8MM device class)

Use the 8MM device class when you are using 8 mm tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--------------------------->

>--LIBRary--=--library_name--DEVType--=--8MM-------------------->

   .-WORM--=--No------.  .-FORMAT--=--DRIVE-----.
>--+------------------+--+---------------------+--------------->
   '-WORM--=--+-No--+-'  '-FORMAT--=--+-DRIVE-+-'
              '-Yes-'                 +-8200--+
                                      +-8200C-+
                                      +-8500--+
                                      +-8500C-+
                                      +-8900--+
                                      +-AIT---+
                                      +-AITC--+
                                      +-M2----+
                                      +-M2C---+
                                      +-SAIT--+
                                      +-SAITC-+
                                      +-VXA2--+
                                      +-VXA2C-+
                                      +-VXA3--+
                                      '-VXA3C-'

>--+---------------------+-------------------------------------->
   '-ESTCAPacity--=--size-'

   .-PREFIX--=--ADSM-------------------.
>--+---------------------------------+------------------------->
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)
: Specifies the name of the defined library object that contains the 8 mm tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=8MM (Required)
: Specifies that the 8MM device type is assigned to the device class. 8MM indicates that 8 mm tape devices are assigned to this device class.

WORM

Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. The field can contain one of the following values:

Yes
: Specifies that the drives use WORM media.

No
: Specifies that the drives do not use WORM media.

Note: If you select Yes, the only options available for the FORMAT parameter are:

- DRIVE
- AIT
- AITC

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for 8 mm devices:

Table 1. Recording format and default estimated capacity for 8 mm tape

Format **Medium Type**	**Estimated Capacity**	**Description**
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
8200	2.3 GB	Uncompressed (standard) format, using standard 112-meter tape cartridges
8200C	See note 3.5 GB 4.6 GB	Compressed format, using standard 112-meter tape cartridges
8500 15m 15m 15m 54m 54m 54m 112m 112m 112m 160m XL	See note 600 MB 600 MB 600 MB 2.35 GB 2.35 GB 2.35 GB 5 GB or 10.0 GB 5 GB or 10.0 GB 5 GB or 10.0 GB 7 GB	Drives (Read Write) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW)

Format Medium Type	 Estimated Capacity	Description
8500C	See note	Drives (Read Write)
15m	1.2 GB	Eliant 820 (RW)
15m	1.2 GB	Exabyte 8500/8500C (RW)
15m	1.2 GB	Exabyte 8505 (RW)
54m	4.7 GB	Eliant 820 (RW)
54m	4.7 GB	Exabyte 8500/8500C (RW)
54m	4.7 GB	Exabyte 8505 (RW)
112m	5 GB or 10.0 GB	Eliant 820 (RW)
112m	5 GB or 10.0 GB	Exabyte 8500/8500C (RW)
112m	5 GB or 10.0 GB	Exabyte 8505 (RW)
160m XL	7 GB	Eliant 820 (RW)
8900	See note	Drive (Read Write)
15m	–	Mammoth 8900 (R)
54m	–	Mammoth 8900 (R)
112m	–	Mammoth 8900 (R)
160m XL	–	Mammoth 8900 (R)
22m	2.5 GB	Mammoth 8900 (RW)
125m	–	Mammoth 8900 (RW with upgrade)
170m	40 GB	Mammoth 8900 (RW)
AIT	See note	Drive
SDX1–25C	25 GB	AIT, AIT2 and AIT3 drives
SDX1–35C	35 GB	AIT, AIT2 and AIT3 drives
SDX2–36C	36 GB	AIT2 and AIT3 drives
SDX2–50C	50 GB	AIT2 and AIT3 drives
SDX3–100C	100 GB	AIT3, AIT4, and AIT5 drives
SDX3X-150C	150 GB	AIT3-Ex, AIT4, and AIT5 drives
SDX4–200C	200 GB	AIT4 and AIT5 drives
SDX5-400C	400 GB	AIT5 drive
AITC	See note	Drive
SDX1–25C	50 GB	AIT, AIT2 and AIT3 drives
SDX1–35C	91 GB	AIT, AIT2 and AIT3 drives
SDX2–36C	72 GB	AIT2 and AIT3 drives
SDX2–50C	130 GB	AIT2 and AIT3 drives
SDX3–100C	260 GB	AIT3, AIT4, and AIT5 drives
SDX3X-150C	390 GB	AIT3-Ex, AIT4, and AIT5 drives
SDX4–200C	520 GB	AIT4 and AIT5 drives
SDX5-400C	1040 GB	AIT5 drive
M2	See note	Drive (Read Write)
75m	20.0 GB	Mammoth II (RW)
150m	40.0 GB	Mammoth II (RW)
225m	60.0 GB	Mammoth II (RW)
M2C	See note	Drive (Read Write)
75m	50.0 GB	Mammoth II (RW)
150m	100.0 GB	Mammoth II (RW)
225m	150.0 GB	Mammoth II (RW)
SAIT	See note	Drive (Read Write)
	500 GB	Sony SAIT1–500(RW)
SAITC	See note	Drive (Read Write)
	1300 GB (1.3 TB)	Sony SAIT1–500(RW)

Format Medium Type	 Estimated Capacity	Description
VXA2 V6 (62m) V10 (124m) V17 (170m)	See note 20 GB 40 GB 60 GB	Drive (Read Write) VXA–2
VXA2C V6 (62m) V10 (124m) V17 (170m)	See note 40 GB 80 GB 120 GB	Drive (Read Write) VXA–2
VXA3 X6 (62m) X10 (124m) X23 (230m)	See note 40 GB 86 GB 160 GB	Drive (Read Write) VXA–3
VXA3C X6 (62m) X10 (124m) X23 (230m)	See note 80 GB 172 GB 320 GB	Drive (Read Write) VXA–3
Note: The actual capacities might vary depending on which cartridges and drives are used. • For the M2C format, the normal compression ratio is 2.5:1. • For the AITC and SAITC formats, the normal compression ratio is 2.6:1.		

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

For more information about the default estimated capacity for 8 mm tapes, see Table 1.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

Example: Define an 8 mm device class

Define a device class that is named 8MMTAPE for an 8 mm device in a library named AUTO. The format is DRIVE, mount limit is 2, mount retention is 10, tape volume prefix is named ADSMVOL, and the estimated capacity is 6 GB.

```
define devclass 8mmtape devtype=8mm library=auto
format=drive mountlimit=2 mountretention=10
prefix=adsmvol estcapacity=6G
```

DEFINE DEVCLASS (Define a CENTERA device class)

Use the CENTERA device class when you are using EMC Centera storage devices. The CENTERA device type uses files as volumes to store data sequentially. It is similar to the FILE device class.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--DEVType--=--CENTERA------>

                      .-,----------.
              (1)     V            |
>--HLAddress------=----ip_address-+-?PEA_file------------------>

   .-MINCAPacity--=--100M-.  .-MOUNTLimit--=--1------.
>--+----------------------+--+----------------------+---------><
   '-MINCAPacity--=--size-'  '-MOUNTLimit--=--number-'
```

Notes:

1. For each Centera device class, you must specify one or more IP addresses. However, a Pool Entry Authorization (PEA) file name and path are optional, and up to one PEA file specification can follow the IP addresses. Use the "?" character to separate the PEA file name and path from the IP addresses.

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

DEVType=CENTERA (Required)
: Specifies that the Centera device type is assigned to this device class. All volumes that belong to a storage pool that is defined to this device class are logical volumes that are a form of sequential access media.

HLAddress
: Specifies one ore more IP addresses for the Centera storage device and, optionally, the name and path of one Pool Entry Authorization (PEA) file. Specify the IP addresses with the dotted decimal format (for example, 9.10.111.222). A Centera device might have multiple IP addresses. If multiple IP addresses are specified, then the store or retrieve operation attempts a connection by using each IP address that is specified until a valid address is found.

  AIX The PEA file name and path name are case-sensitive.

  If you append the name and path of a PEA file, ensure that the file is stored in a directory on the system that runs the server. Separate the PEA file name and path from the IP address with the "?" character, for example: Windows

  ```
  HLADDRESS=9.10.111.222,9.10.111.223?c:\controlFiles\TSM.PEA
  ```

  AIX

  ```
  HLADDRESS=9.10.111.222,9.10.111.223?/user/ControlFiles/TSM.PEA
  ```

  Specify only one PEA file name and path for each device class definition. If you specify two different Centera device classes that point to the same Centera storage device and if the device class definitions contain different PEA file names and paths, the server uses the PEA file that is specified in the device class HLADDRESS parameter that was first used to open the Centera storage device.
  Tips:

  1. The server does not include a PEA file during installation. If you do not create a PEA file, the server uses the Centera default profile, which can allow applications to read, write, delete, purge, and query data on a Centera storage device. To provide tighter control, create a PEA file with the command-line interface that is provided by EMC Centera. For details about Centera authentication and authorization, refer to the EMC Centera *Programmer's Guide*.
  2. You can also specify the PEA file name and path in an environment variable with the syntax CENTERA_PEA_LOCATION=filePath_ fileName. The PEA file name and path that is specified with this environment variable apply to all Centera clusters. If you use this variable, you do not have to specify the PEA file name and path with the HLADDRESS parameter.

MINCAPacity
: Specifies the minimum size for Centera volumes that are assigned to a storage pool in this device class. This value represents the minimum amount of data that is stored on a Centera volume before the server marks it full. Centera volumes continue to accept data until the minimum amount of data is stored. This parameter is optional.

  Specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The default value is 100 MB (MINCAPACITY=100M). The minimum value that is allowed is 1 MB (MINCAPACITY=1M). The maximum value that is allowed is 128 GB (MINCAPACITY=128G).

MOUNTLimit

Specifies the maximum number of files that can be simultaneously open for input and output. The default value is 1. This parameter is optional. You can specify any number from 0 or greater; however, the sum of all mount limit values for all device classes that are assigned to the same Centera device must not exceed the maximum number of sessions that are allowed by Centera.

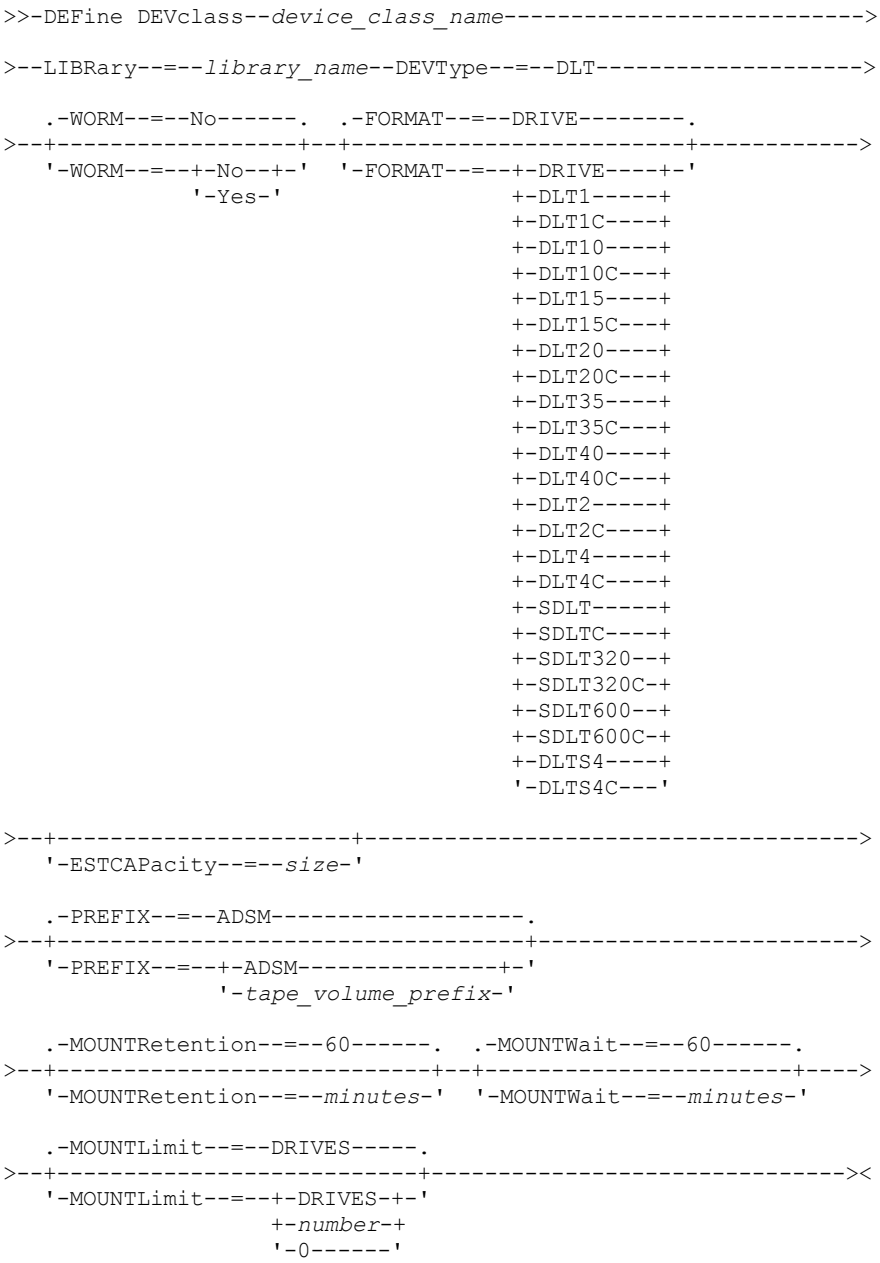
DEFINE DEVCLASS (Define a DLT device class)

Use the DLT device class when you are using DLT tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)
Specifies the name of the defined library object that contains the DLT tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=DLT (Required)
Specifies that the DLT device type is assigned to the device class. DLT indicates that DLT tape devices are assigned to this device class.

WORM
Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. The field can contain one of the following values:

Yes
Specifies that the drives use WORM media.

No
Specifies that the drives do not use WORM media.

Note: Support for DLT WORM media is available only for SDLT-600, Quantum DLT-V4, and Quantum DLT-S4 drives in manual, SCSI, and ACSLS libraries.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for DLT devices:

Table 1. Recording format and default estimated capacity for DLT

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
DLT1	40.0 GB	Uncompressed format, using only CompacTape III cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT1C	See note 1. 80.0 GB	Compressed format, using only CompacTape III cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT10	10.0 GB	Uncompressed format, using only CompacTape III cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT10C	See note 1. 20.0 GB	Compressed format, using only CompacTape III cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT15	15.0 GB	Uncompressed format, using only CompacTape IIIxt cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT15C	See note 1. 30.0 GB	Compressed format, using only CompacTape IIIxt cartridges Valid with DLT4000, DLT7000, and DLT8000 drives

Format	Estimated Capacity	Description
DLT20	20.0 GB	Uncompressed format, using only CompacTape IV cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT20C	See note 1. 40.0 GB	Compressed format, using only CompacTape IV cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT35	35.0 GB	Uncompressed format, using only CompacTape IV cartridges Valid with DLT7000 and DLT8000 drives
DLT35C	See note 1. 70.0 GB	Compressed format, using only CompacTape IV cartridges Valid with DLT7000 and DLT8000 drives
DLT40	40.0 GB	Uncompressed format, using CompacTape IV cartridges Valid with a DLT8000 drive
DLT40C	See note 1. 80.0 GB	Compressed format, using CompacTape IV cartridges Valid with a DLT8000 drive
DLT2	80.0 GB	Uncompressed format, using Quantum DLT tape VS1 media
DLT2C	See note 1. 160.0 GB	Compressed format, using Quantum DLT tape VS1 media
DLT4	160.0 GB	Uncompressed format, using Quantum DLTtape VS1 cartridges. Valid with Quantum DLT-V4 drive
DLT4C	See note 1. 320.0 GB	Compressed format, using Quantum DLTtape VS1 cartridges. Valid with Quantum DLT-V4 drive
SDLT See note 2.	100.0 GB	Uncompressed format, using Super DLT Tape 1 cartridges Valid with a Super DLT drive
SDLTC See note 2.	See note 1. 200.0 GB	Compressed format, using Super DLT Tape 1 cartridges Valid with a Super DLT drive
SDLT320 See note 2.	160.0 GB	Uncompressed format, using Quantum SDLT I media Valid with a Super DLT drive
SDLT320C See note 2.	See note 1. 320.0 GB	Compressed format, using Quantum SDLT I media Valid with a Super DLT drive
SDLT600	300.0 GB	Uncompressed format, using SuperDLTtape-II media Valid with a Super DLT drive
SDLT600C	See note 1. 600.0 GB	Compressed format, using SuperDLTtape-II media Valid with a Super DLT drive
DLTS4	800 GB	Uncompressed format, using Quantum DLT S4 media. Valid with a DLT-S4 drive
DLTS4C	See note 1. 1.6 TB	Compressed format, using Quantum DLT S4 media. Valid with a DLT-S4 drive

Format	Estimated Capacity	Description

Note:

1. Depending on the effectiveness of compression, the actual capacity might be greater than the listed value.
2. IBM Spectrum Protect™ does not support a library that contains both Backward Read Compatible (BRC) SDLT and Non-Backward Read Compatible (NBRC) SDLT drives.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

For more information about estimated capacities, see Table 1.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
: Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
  Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
: Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
: Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DEFINE DEVCLASS (Define an ECARTRIDGE device class)

Use the ECARTRIDGE device class when you are using StorageTek drives such as the StorageTek T9840 or T10000.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see DEFINE DEVCLASS (Define an ECARTRIDGE device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name---------------------------->

>--LIBRary--=--library_name--DEVType--=--ECARTridge------------->

                                                    (1)
   .-LBProtect--=--No------------.  .-WORM--=--No------.
>--+-----------------------------+--+------------------+-------->
   '-LBProtect--=--+-READWrite-+-'  '-WORM--=--+-No--+-'
                   +-WRITEOnly-+               '-Yes-'
                   '-No--------'

   .-FORMAT--=--DRIVE---------.
>--+--------------------------+--+----------------------+------->
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--size-'
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

   .-PREFIX--=--ADSM-------------------.
>--+---------------------------------+------------------------->
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'
```

```
   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+--------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'

                                (1) (2)
   .-DRIVEEncryption--=--ALLOW---------.
>--+-----------------------------------+------------------------><
   '-DRIVEEncryption--=--+-ON-------+--'
                         +-ALLOW----+
                         +-EXTernal-+
                         '-OFF------'
```

Notes:

1. You cannot specify both WORM=Yes and DRIVEENCRYPTION=ON.
2. You can use drive encryption only for Oracle StorageTek T10000B drives with a format value of DRIVE, T10000B, or T10000B-C, for Oracle StorageTek T10000C drives with a format value of DRIVE, T10000C or T10000C-C, and for Oracle StorageTek T10000D drives with a format value of DRIVE, T10000D and T10000D-C.

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)
: Specifies the name of the defined library object that contains the ECARTRIDGE tape drives that can be used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=ECARTridge (Required)
: Specifies that the ECARTRIDGE device type is assigned to the device class. ECARTRIDGE indicates that a specific type of cartridge tape device (StorageTek) is assigned to this device class.

LBProtect

: Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

  The default is NO.

  The following values are possible:

  READWrite
  : Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect™ and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

    When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

  WRITEOnly
  : Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

  No
  : Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

  Restriction: Logical block protection is supported only on Oracle StorageTek T10000C and Oracle StorageTek T10000D drives.

WORM

Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. The field can contain one of the following values:

Yes
: Specifies that the drives use WORM media.

No
: Specifies that the drives do not use WORM media.

Restriction: If you select Yes, the only options that are available for the FORMAT parameter are:

- DRIVE
- T9840C
- T9840C-C
- T9840D
- T9840D-C
- T10000A
- T10000A-C
- T10000B
- T10000B-C
- T10000C
- T10000C-C
- T10000D
- T10000D-C

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

Important: If you specify DRIVE for a device class that has non-compatible sequential access devices, then you must mount volumes on devices that are capable of reading or writing the format that is established when the volume was first mounted. This can cause delays if the only sequential access device that can access the volume is already in use.
The following table lists the recording formats and estimated capacities for ECARTRIDGE devices:

Table 1. Recording formats and default estimated capacities for ECARTRIDGE tapes

Format	Estimated capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge

Format	Estimated capacity	Description
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

Notes:

- Some formats use a tape drive hardware compression feature. Depending on the effectiveness of compression, the actual capacity might be double or more than the listed value.
- T10000A drives can read and write the T10000A format only. T10000B drives can read, but cannot write, the T10000A format. T10000C drives can read, but cannot write, the T10000A and T10000B formats. T10000D drives can read, but cannot write, the T10000A, T10000B, and T10000C formats.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption

Specifies whether drive encryption is allowed. This parameter is optional. The default is ALLOW.
Restrictions:

1. You can use drive encryption only for the following drives:
   - Oracle StorageTek T10000B drives that have a format value of DRIVE, T10000B, or T10000B-C
   - Oracle StorageTek T10000C drives that have a format value of DRIVE, T10000C, or T10000C-C
   - Oracle StorageTek T10000D drives that have a format value of DRIVE, T10000D, or T10000D-C
2. You cannot specify IBM Spectrum Protect as the key manager for drive encryption of write once, read many (WORM) media. You cannot specify both WORM=Yes and DRIVEENCRYPTION=ON.
3. If encryption is enabled for a device class, and the device class is associated with a storage pool, the storage pool should not share a scratch pool with other device classes that cannot be encrypted. If a tape is encrypted, and you plan to use it on a drive that cannot be encrypted, you must manually relabel the tape before it can be used on that drive.

ON

Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes are not encrypted. For example, back up sets, export volumes, and database backup volumes are not encrypted.) If you specify ON and you enable another method of encryption, drive encryption is not allowed and backup operations fail.

ALLOW

Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if another method of encryption is enabled.

EXTernal

Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive. When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption. By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF
: Specifies that drive encryption is not allowed. If you enable another method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

DEFINE DEVCLASS (Define a FILE device class)

Use the FILE device class when you are using files on magnetic disk storage as volumes that store data sequentially (as on tape).

AIX Linux The FILE device class does not support EXTERNAL libraries.

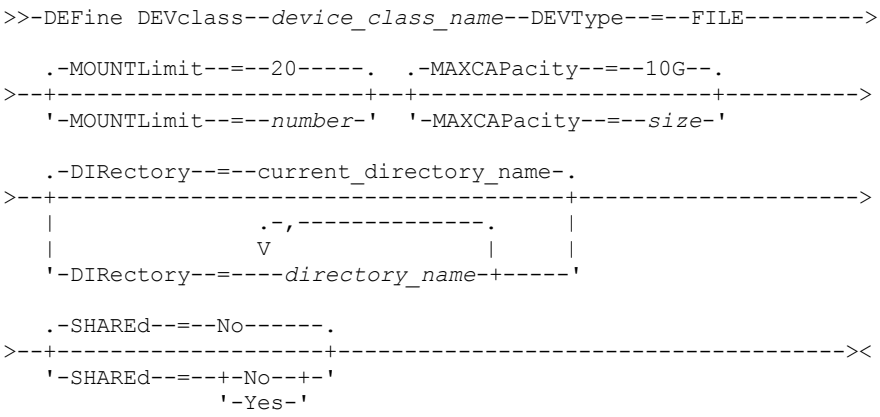
Windows The FILE device class does not support EXTERNAL or Remote Storage Manager libraries.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see DEFINE DEVCLASS (Define a FILE device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

DEVType=FILE (Required)
: Specifies that the FILE device type is assigned to the device class. FILE indicates that a file is assigned to this device class. When the server must access a volume that belongs to this device class, it opens a file and reads or writes file data.

  A file is a form of sequential-access media.

MOUNTLimit
: Specifies the maximum number of files that can be simultaneously open for input and output. This parameter is optional. The default value is 20. You can specify a number from 0 to 4096.

  Windows If the device class is shared with a storage agent (by specifying the SHARED=YES parameter), drives are defined or deleted to match the mount limit value.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

MAXCAPacity
: Specifies the maximum size of any data storage files that are defined to a storage pool in this device class.

  The value of the MAXCAPACITY parameter is also used as the unit of allocation when storage pool space triggers create volumes. The default value is 10 GB (MAXCAPACITY=10G). The value that is specified must be less than or equal to the

maximum supported size of a file on the target file system.

Specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The minimum size is 1 MB (MAXCAPACITY=1M). If you are defining a FILE device class for database-backup volumes, specify a value for MAXCAPACITY that is appropriate for the size of the database and that minimizes the number of database volumes.

AIX Linux Do not define a MAXCAPACITY value greater than 640M when this file is for REMOVABLEFILE CD support. A value less than a CD's usable space (650 MB) enables a one-to-one match between files from the FILE device class and copies that are on CD.

DIRectory
Specifies the directory location or locations of the files that are used in this device class. Enclose the entire list of directories within quotation marks, and use commas to separate individual directory names. Special characters (for example, blank spaces) are allowed within directory names. For example, the directory list "abc def,xyz" contains two directories: abc def and xyz.

This parameter is optional.

AIX Linux The default is the current working directory of the server at the time the command is issued.

Windows The default is the current working directory of the server at the time the command is issued. Windows registry information is used to determine the default directory.

By specifying a directory name or names, you identify the location where the server places the files that represent storage volumes for this device class.

For NetApp SnapLock support (storage pools with RECLAMATIONTYPE=SNAPLOCK, which are going to use this device class), the directory, or directories that are specified with DIRECTORY parameter must point to the directory or directories on the NetApp SnapLock volumes.

AIX Linux While the command is processed, the server expands the specified directory name or names into their fully qualified forms, starting from the root directory.

If the server must allocate a scratch volume, it creates a new file in one of these directories. (The server can choose any of the directories in which to create new scratch volumes.) For scratch volumes used to store client data, the file that is created by the server has a file name extension of .bfs. For scratch volumes used to store export data, a file name extension of .exp is used.

AIX Linux For example, if you define a device class with a directory of tsmstor and the server needs a scratch volume in this device class to store export data, the file that the server creates might be named /tsmstor/00566497.exp.

Windows For example, if you define a device class with a directory of c:\server and the server needs a scratch volume in this device class to store export data, the file that the server creates might be named c:\server\00566497.exp.

Important: You must ensure that storage agents can access newly created FILE volumes. Failure of the storage agent to access a FILE volume can cause operations to be retried on a LAN-only path or to fail. For more information, see the description of the DIRECTORY parameter in DEFINE PATH (Define a path).
Tip: If you specify multiple directories for a device class, ensure that the directories are associated with separate file systems. Space trigger functions and storage pool space calculations take into account the space that remains in each directory. If you specify multiple directories for a device class and the directories are in the same file system, the server calculates space by adding values that represent the space that remains in each directory. These space calculations are inaccurate. Rather than choosing a storage pool with sufficient space for an operation, the server might choose the wrong storage pool and run out of space prematurely. For space triggers, an inaccurate calculation might result in a failure to expand the space available in a storage pool. Failure to expand space in a storage pool is one of the conditions that can cause a trigger to become disabled. If a trigger is disabled because the space in a storage pool could not be expanded, you can re-enable the trigger by issuing the following command: `update spacetrigger stg`. No further changes are required to the space trigger.

SHAREd
Specifies that this FILE device class is shared between the server and one or more storage agents. To prepare for sharing, a library is automatically defined along with a number of drives corresponding to the MOUNTLIMIT parameter value. The drive names are the name of the library plus a number from 1 to the mount limit number. For example, if the library name is FILE and the mount limit is set to 4, the drives are named FILE11, FILE12, FILE13, FILE14.

For information about prerequisites when storage is shared by the server and storage agent, see IBM® Support Portal for IBM Spectrum Protect™.

Example: Define a FILE device class with multiple directories

Define a device class that specifies multiple directories.

AIX

```
define devclass multidir devtype=file
   directory=/usr/xyz,/usr/abc,/usr/uvw
```

Linux

```
define devclass multidir devtype=file
   directory=/opt/xyz,/opt/abc,/opt/uvw
```

Windows

```
define devclass multidir devtype=file
   directory=e:\xyz,f:\abc,g:\uvw
```

Example: Define a FILE device class with a 50 MB capacity

Define a device class named PLAINFILES with a FILE device type and a maximum capacity of 50 MB.

```
define devclass plainfiles devtype=file
maxcapacity=50m
```

AIX | Windows

DEFINE DEVCLASS (Define a GENERICTAPE device class)

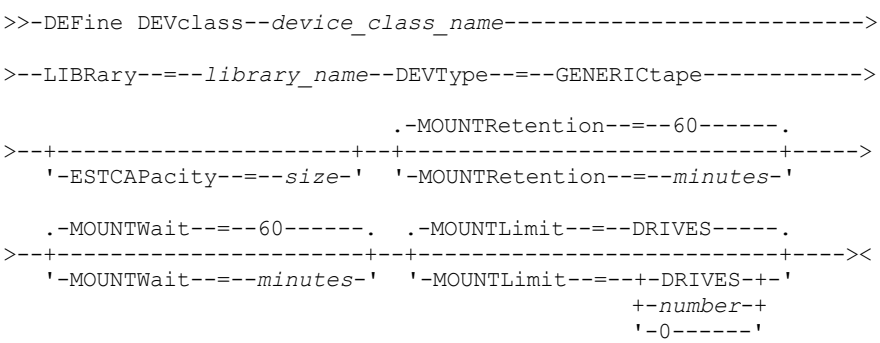
Use the GENERICTAPE device class for tape drives that are supported by operating system device drivers.

When you use this device type, the server does not recognize either the type of device or the cartridge recording format. Because the server does not recognize the type of device, if an I/O error occurs, error information is less detailed compared to error information for a specific device type (for example, 8MM). When you define devices to the server, do not mix various types of devices within the same device type.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

: Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

: For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=GENERICtape (Required)
Specifies that the GENERICTAPE device type is assigned to the device class. GENERICTAPE indicates that the volumes for this device class are used in tape drives that are supported by the operating system's tape device driver.

The server recognizes that the media can be removed and that more media can be inserted, subject to limits set with the MOUNTLIMIT parameter for the device class and the MAXSCRATCH parameter for the storage pool.

Volumes in a device class with device type GENERICTAPE are sequential access volumes.

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

Specify a capacity appropriate to the particular tape drive that is being used.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DEFINE DEVCLASS (Define an LTO device class)

Use the LTO device class when you are using LTO tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Notes:

1. You cannot specify both WORM=Yes and DRIVEENCRYPTION=ON.
2. IBM Spectrum Protect™ server supports LTO-2 tape drives; however, IBM® Tape Device drivers do not. In the event of an issue with the LTO-2 drive, the preferred corrective action is to upgrade your tape drive hardware to a higher generation

drive, then install the latest version of the device driver.
3. Drive encryption is supported only for LTO-4 and higher generation LTO drives and media.

Parameters

device_class_name (Required)
Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)
Specifies the name of the defined library object that contains the LTO tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=LTO (Required)
Specifies that the linear tape open (LTO) device type is assigned to the device class.

LBProtect

Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

The default is NO.

The following values are possible:

READWrite
Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

WRITEOnly
Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

No
Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

Restriction:
Restrictions apply to logical block protection (LBP):

- At the LTO-5 level, LBP is supported only on IBM LTO-5.
- Starting with LTO-6, LBP is supported by all LTO drive vendors.

WORM
Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. The field can contain one of the following values:

Yes
Specifies that the drives use WORM media.

No
Specifies that the drives do not use WORM media.

Note:

1. To use WORM media in a library, all the drives in the library must be WORM capable.
2. You cannot specify IBM Spectrum Protect as the key manager for drive encryption of WORM (write once, read many) media. (Specifying both WORM=Yes and DRIVEENCRYPTION=ON is not supported.)

FORMAT

Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

If you are considering mixing different generations of LTO media and drives, be aware of the following restrictions.

Table 1. Read - write capabilities for different generations of LTO drives

Drives	Generation 3 media	Generation 4 media	Generation 5 media	Generation 6 media	Generation 7 media	Generation M8 media	Generation 8 media
Generation 3 [1]	Read and write	n/a	n/a	n/a	n/a	n/a	n/a
Generation 4 [1]	Read and write	Read and write	n/a	n/a	n/a	n/a	n/a
Generation 5 [1]	Read only	Read and write	Read and write	n/a	n/a	n/a	n/a
Generation 6 [1]	n/a	Read only	Read and write	Read and write	n/a	n/a	n/a
Generation 7[1]			Read only	Read and write	Read and write	n/a	n/a
Generation 8[2]	n/a	n/a	n/a	n/a	Read and write	Read and write	Read and write

[1] If a storage pool volume can only be read by a tape drive, ensure that the attributes of the storage pool volume are set to read only.

[2] LTO-8 drives have two media types: LTO-M8 media and LTO-8 media. Both media types are used only in LTO-8 tape drives.

The following table lists the recording formats and estimated capacities for LTO devices:

Table 2. Recording format and default estimated capacity for LTO

Format	Estimated capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
ULTRIUM2	200 GB	Uncompressed (standard) format, using Ultrium 2 cartridges
ULTRIUM2C	See note 400 GB	Compressed format, using Ultrium 2 cartridges
ULTRIUM3	400 GB	Uncompressed (standard) format, using Ultrium 3 cartridges
ULTRIUM3C	See note 800 GB	Compressed format, using Ultrium 3 cartridges
ULTRIUM4	800 GB	Uncompressed (standard) format, using Ultrium 4 cartridges

Format	Estimated capacity	Description
ULTRIUM4C	See note 1.6 TB	Compressed format, using Ultrium 4 cartridges
ULTRIUM5	1.5 TB	Uncompressed (standard) format, using Ultrium 5 cartridges
ULTRIUM5C	Varied, as described in note	Compressed format, using Ultrium 5 cartridges
ULTRIUM6	2.5 TB	Uncompressed (standard) format, using Ultrium 6 cartridges
ULTRIUM6C	Varied, as described in note	Compressed format, using Ultrium 6 cartridges
ULTRIUM7	6 TB	Uncompressed (standard) format, using Ultrium 7 cartridges
ULTRIUM7C	Varied, as described in note	Compressed format, using Ultrium 7 cartridges
ULTRIUM8	12 TB for LTO-8 media 9 TB for LTO-M8 media	Uncompressed (standard) format, using Ultrium M8 or Ultrium 8 cartridges
ULTRIUM8C	Varied, as described in note	Compressed format, using Ultrium M8 or Ultrium 8 cartridges
Note: If this format uses the tape-drive hardware-compression feature, depending on the effectiveness of compression, the actual capacity is varied.		

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

For more information about estimated capacities, see Table 2.

PREFIX
Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption

Specifies whether drive encryption is allowed. This parameter is optional. The default is ALLOW. Drive encryption is supported only for LTO-4 and higher generation drives and media.
Restriction: If encryption is enabled for a device class, and the device class is associated with a storage pool, the storage pool should not share a scratch pool with other device classes that cannot be encrypted. If a tape is encrypted, and you plan to use it on a drive that cannot be encrypted, you must manually relabel the tape before it can be used on that drive.

ON

Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes are not encrypted. For example, back up sets, export volumes, and database backup volumes are not encrypted.) If you specify ON and you enable another method of encryption, drive encryption is not allowed and backup operations fail.
Note: You cannot specify IBM Spectrum Protect as the key manager for drive encryption of WORM (write once, read many) media. (Specifying both WORM=Yes and DRIVEENCRYPTION=ON is not supported.)

ALLOW

Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if another method of encryption is enabled.

EXTERNAL

Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive. When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption. By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF

Specifies that drive encryption is not allowed. If you enable another method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

Example: Define an LTO device class

Define a device class that is named LTOTAPE for an LTO drive in a library named LTOLIB. The format is ULTRIUM, mount limit is 12, mount retention is 5, tape volume prefix is named SMVOL, and the estimated capacity is 100 GB.

```
define devclass ltotape devtype=lto library=ltolib
format=ultrium mountlimit=12 mountretention=5
prefix=smvol estcapacity=100G
```

DEFINE DEVCLASS (Define a NAS device class)

Use the NAS device class when you are using NDMP (Network Data Management Protocol) operations to back up network-attached storage (NAS) file servers. The device class is for drives that are supported by the NAS file server for backups.

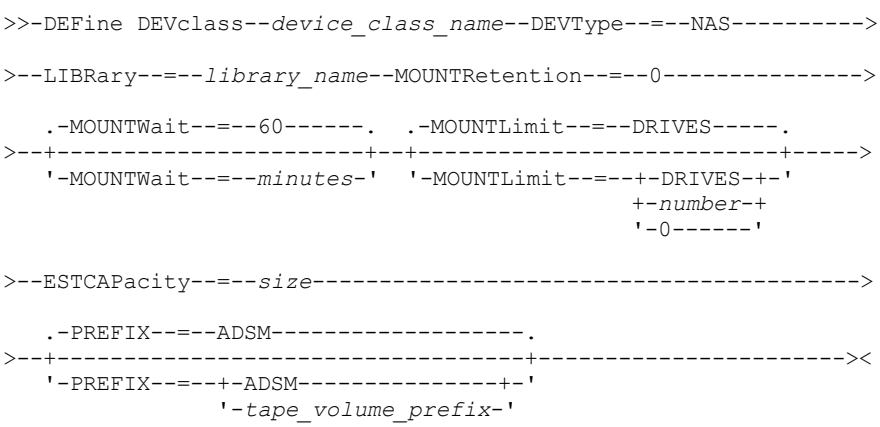
AIX Linux The NAS device class does not support EXTERNAL libraries.

Windows The NAS device class does not support EXTERNAL or Remote Storage Manager libraries.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

DEVType=NAS (Required)
: Specifies that the network-attached storage (NAS) device type is assigned to the device class. The NAS device type is for drives that are attached to and used by a NAS file server for backup of NAS file systems.

LIBRary (Required)
: Specifies the name of the defined library object that contains the SCSI tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

MOUNTRetention=0 (Required)
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. Zero (0) is the only supported value for device classes with DEVType=NAS.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
: Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
: Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
: Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
: Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

ESTCAPacity (Required)
: Specifies the estimated capacity for the volumes that are assigned to this device class.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

PREFIX
: Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

Example: Define a NAS device class

Define a device class that is named NASTAPE for a NAS drive in a library named NASLIB. The mount limit is DRIVES, mount retention is 0, tape volume prefix is named SMVOL, and the estimated capacity is 200 GB.

```
define devclass nastape devtype=nas library=naslib
mountretention=0 mountlimit=drives
prefix=smvol estcapacity=200G
```

DEFINE DEVCLASS (Define a REMOVABLEFILE device class)

Use the REMOVABLEFILE device class for removable media devices that are attached as local, removable file systems.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--------------------------->

>--LIBRary---=--library_name--DEVType--=--REMOVABLEfile---------->

   .-MAXCAPacity--=--space_remaining-.
>--+---------------------------------+-------------------------->
   '-MAXCAPacity--=--size------------'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)
: Specifies the name of the defined library object that contains the removable media drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

DEVType=REMOVABLEfile (Required)
: Specifies that the REMOVABLEFILE device type is assigned to the device class. REMOVABLEFILE indicates that the volumes for this device class are files on local, removable media.

  Volumes in a device class with device type REMOVABLEFILE are sequential access volumes.

  Use the device manufacturer's utilities to format (if necessary) and label the media. The label on the media must meet the following restrictions:

  - The label can have no more than 11 characters.
  - The volume label and the name of the file on the volume must match exactly.
  - AIX Windows The MAXCAPACITY parameter value must be specified at less than the capacity of the media.

MAXCAPacity
: Specifies the maximum size of any volumes that are defined to a storage pool categorized by this device class. This parameter is optional.

  The MAXCAPACITY parameter must be set at less value than the capacity of the media. For CD media, the maximum capacity can be no greater than 650 MB.

  AIX Windows Because the server opens only one file per physical removable medium, specify a capacity that enables one file to make full use of your media capacity.

  space_remaining
  : The default maximum capacity is the space that remains on the media after it is first used.

  size
  : You must specify this value as an integer followed by K (kilobytes), M (megabytes), G (gigabytes), or T (terabytes).

  For example, MAXCAPACITY=5M specifies that the maximum capacity for a volume in this device class is 5 MB. The smallest value that is allowed is 1 MB (that is, MAXCAPACITY=1M).

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DEFINE DEVCLASS (Define a SERVER device class)

Use the SERVER device class to use storage volumes or files that are archived in another IBM Spectrum Protect™ server.

If data retention protection is activated with the SET ARCHIVERETENTIONPROTECTION command, you cannot define a server device class.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--DEVType--=--SERVER------->

                                .-MAXCAPacity--=--500M-.
>--SERVERName--=--server_name--+----------------------+--------->
                                '-MAXCAPacity--=--size-'

   .-MOUNTLimit--=--1------.  .-MOUNTRetention--=--60------.
>--+---------------------+--+---------------------------+---->
   '-MOUNTLimit--=--number-'  '-MOUNTRetention--=--minutes-'

   .-PREFIX--=--ADSM--------------.
>--+-----------------------------+---------------------------->
   '-PREFIX--=--+-ADSM----------+-'
                '-volume_prefix-'
```

```
   .-RETRYPeriod--=--10--------------------.
>--+---------------------------------------+--------------------><
   '-RETRYPeriod--=--retry_value_(minutes)-'

   .-RETRYInterval--=--30--------------------.
>--+---------------------------------------+-----------------><
   '-RETRYInterval--=--retry_value_(seconds)-'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

DEVType=SERVER (Required)
: Specifies a remote connection that supports virtual volumes.

SERVERName (Required)
: Specifies the name of the server. The SERVERNAME parameter must match a defined server.

MAXCAPacity
: Specifies the maximum size for objects that are created on the target server; the default for this value is 500M. This parameter is optional.

  500M
  : Specifies that the maximum capacity is 500M (500 MB).

  size
  : Specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The minimum value that is allowed is 1 MB (MAXCAPACITY=1M).

MOUNTLimit
: Specifies the maximum number of simultaneous sessions between the source server and the target server. Any attempts to access more sessions than indicated by the mount limit cause the requester to wait. This parameter is optional. The default value is 1. You can specify a number 1 - 4096.
  The following are possible values:

  1
  : Specifies that only one session between the source server and the target server is allowed.

  number
  : Specifies the number of simultaneous sessions between the source server and the target server.

MOUNTRetention
: Specifies the number of minutes to retain an idle connection with the target server before the connection closes. This parameter is optional. The default value is 60. You can specify a number 0 - 9999.
  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

PREFIX
: Specifies the beginning portion of the high-level archive file name on the target server. This parameter is optional. The default is ADSM. The maximum length of this prefix is 8 characters.

  If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

  Values that are specified for this parameter must meet the following conditions:

  - The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

    ```
    AB.CD2.E
    ```

  - The qualifiers must be separated by a single period.
  - The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

  An example of a high-level archive file name that uses the default prefix is ADSM.volume1.

RETRYPeriod
: Specifies the retry period in minutes. The retry period is the interval during which the server attempts to contact a target server if there is a suspected communications failure. This parameter is optional. You can specify a number 0 - 9999. The default value is 10 minutes.

RETRYInterval
: Specifies the retry interval in seconds. The retry interval is how often retries are done within a specific time period. This parameter is optional. You can specify a number 1 - 9999. The default value is 30 seconds.

DEFINE DEVCLASS (Define a VOLSAFE device class)

Use the VOLSAFE device type to work with StorageTek VolSafe brand media and drives. This technology uses media that cannot be overwritten. Therefore, do not use these media for short-term backups of client files, the server database, or export tapes.

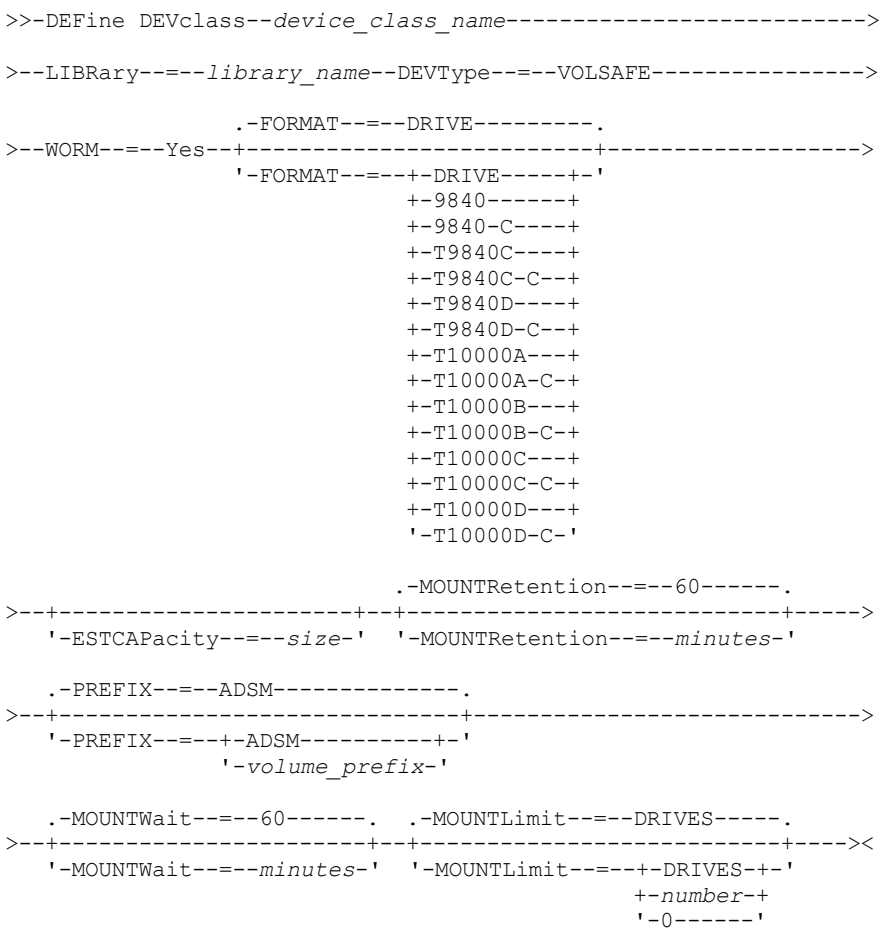
Restrictions:

1. NAS-attached libraries are not supported.
2. VolSafe media and read/write media must be in separate storage pools.
3. Check in cartridges with CHECKLABEL=YES on the CHECKIN LIBVOLUME command.
4. Label cartridges with OVERWRITE=NO on the LABEL LIBVOLUME command. If VolSafe cartridges are labeled more than one time, no additional data can be written to them.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)

Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

Specifies the name of the defined library object that contains the VolSafe drives that can be used by this device class. If any drives in a library are VolSafe-enabled, all drives in the library must be VolSafe-enabled. Consult your hardware documentation to enable VolSafe on the 9840 and T10000 drives.

For information about defining a library object, see DEFINE LIBRARY (Define a library).

DEVType=VOLSAFE (Required)

Specifies that the VOLSAFE device type is assigned to the device class. The label on this type of cartridge can be overwritten one time, which IBM Spectrum Protect™ does when it writes the first block of data. Therefore, it is important to limit the use of the LABEL LIBVOLUME command to one time per volume by using the OVERWRITE=NO parameter.

WORM

Specifies whether the drives use WORM (write once, read many) media. The parameter is required. The value must be Yes.

Yes

Specifies that the drives use WORM media.

FORMAT

Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.

Important: If you specify DRIVE for a device class that has non-compatible sequential access devices, then you must mount volumes on devices that are capable of reading or writing the format that is established when the volume was first mounted. This can cause delays if the only sequential access device that can access the volume is already in use.

The following table lists the recording formats and estimated capacities for VolSafe devices:

Table 1. Recording formats and default estimated capacities for Volsafe media

Format	**Estimated Capacity**	**Description**
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
9840	20 GB	Uncompressed (standard) format, using a 20 GB cartridge with 270 meters (885 feet) of tape
9840-C	See note 80 GB	LZ-1 Enhanced (4:1) compressed format, using an 80 GB cartridge with 270 meters (885 feet) of tape
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

Format	Estimated Capacity	Description
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

For more information about the default estimated capacity for cartridge tapes, see Table 1.

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. The default value is 60 minutes. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

PREFIX
Specifies the beginning portion of the high-level archive file name on the target server. This parameter is optional. The default is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a high-level archive file name that uses the default prefix is ADSM.volume1.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. The default value is 60 minutes. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is DRIVES. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
: Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
: Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
: Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

AIX Linux

DEFINE DEVCLASS - z/OS media server (Define device class for z/OS media server)

Use the DEFINE DEVCLASS command to define a device class for a type of storage device. The server requires that a device class be defined to allow the use of a device. A limited set of device class types is available for devices that are accessed through a z/OS® media server.

- DEFINE DEVCLASS (Define a 3590 device class for z/OS media server)
- DEFINE DEVCLASS (Define a 3592 device class for z/OS media server)
- DEFINE DEVCLASS (Define an ECARTRIDGE device class for z/OS media server)
- DEFINE DEVCLASS (Define a FILE device class for z/OS media server)

Table 1. Commands related to DEFINE DEVCLASS

Command	Description
BACKUP DEVCONFIG	Backs up IBM Spectrum Protect device information to a file.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE DEVCLASS	Deletes a device class.
QUERY DEVCLASS	Displays information about device classes.
UPDATE DEVCLASS (z/OS media server)	Changes the attributes of a device class for storage managed by a z/OS media server.

AIX Linux

DEFINE DEVCLASS (Define a 3590 device class for z/OS media server)

To use a z/OS® media server to access 3590 devices, you must define a 3590 device class. In the device class definition, specify a library that was defined with the LIBTYPE=ZOSMEDIA parameter.

Privilege class

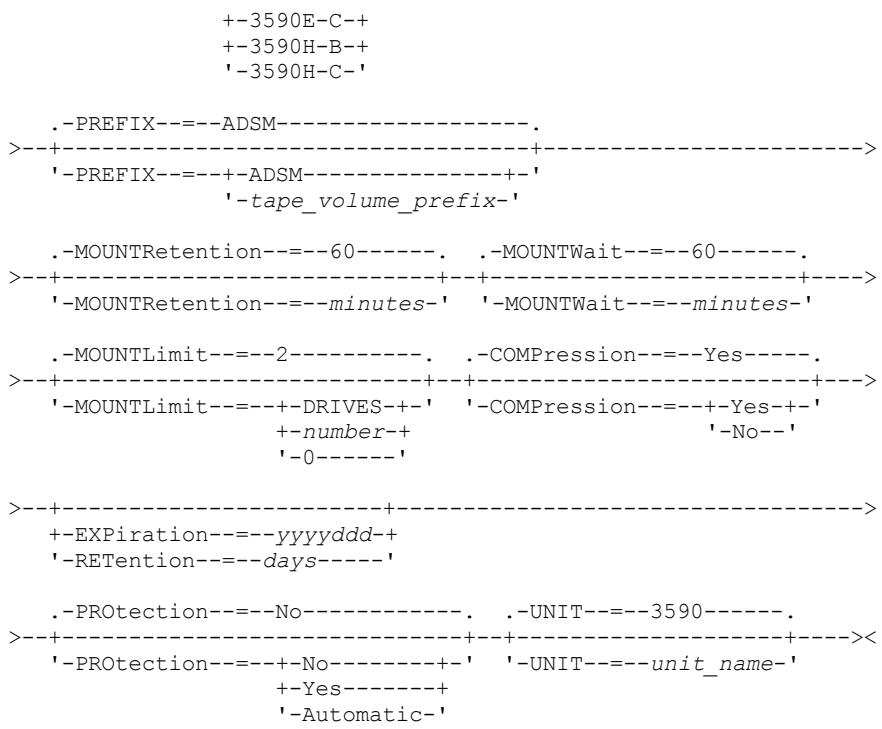
To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name---------------------------->

>--LIBRary--=--zos_media_library--DEVType--=--3590-------------->

                              .-ESTCAPacity--=--9G-------.
>--+-----------------------+--+-------------------------+----->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=----size---'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
```



Parameters

device_class_name (Required)
Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

For information about defining a library, see the DEFINE LIBRARY command.

DEVtype=3590 (Required)
Specifies the 3590 device type is assigned to the device class. 3590 indicates that 3590 cartridge tape devices are assigned to the device class.
Restriction: The z/OS media server supports 256 KB data blocks when writing to 3590 tape drives. Verify that your hardware supports this capability.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. See the following table for the recording formats.

Table 1. Recording formats for 3590

Format	Description
3590B	Uncompressed (basic) format
3590C	Compressed format
3590E-B	Uncompressed (basic) format, similar to the 3590B format
3590E-C	Compressed format, similar to the 3590C format
3590H-B	Uncompressed (basic) format, similar to the 3590B format
3590H-C	Compressed format, similar to the 3590C format
Note: If the format uses the tape drive hardware compression feature the actual capacity can increase, depending on the effectiveness of compression.	

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional. The default estimated capacity for 3590 tapes is 9 GB.

You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

PREFIX
Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. The default value is 60 minutes. Specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait
Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

This parameter is optional. The default value is 60. Specify a number, 1 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is 2.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

You can specify one of the following values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
Specifies that no new transactions can gain access to the storage pool.

COMPression
Specifies whether file compression is used for this device class. This parameter is optional. The default value is YES. You can specify one of the following values:

Yes
Specifies that the data for each tape volume is compressed.

No
Specifies that the data for each tape volume is not compressed.

EXPiration
Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional. There is no default value.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

PROtection
Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. The default value is NO. You can specify one of the following values:

No
Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Automatic
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the server.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT

Specifies an esoteric unit name to specify a group of tape devices that support 3590 tape. This parameter is optional. The default unit name is 3590. The unit name can be up to 8 characters.

AIX | Linux

DEFINE DEVCLASS (Define a 3592 device class for z/OS media server)

To use a z/OS® media server to access 3592 devices, you must define a 3592 device class. In the device class definition, specify a library that was defined with the LIBTYPE=ZOSMEDIA parameter.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name---------------------------->

>--LIBRary--=--zos_media_library--DEVType--=--3592-------------->

   .-FORMAT--=--Drive-------.  .-WORM--=--No------.
>--+------------------------+--+------------------+------------->
   '-FORMAT--=--+-DRIVE---+-'  '-WORM--=--+-Yes-+-'
                +-3592----+               '-No--'
                +-3592C---+
                +-3592-2--+
                +-3592-2C-+
                +-3592-3--+
                +-3592-3C-+
                +-3592-4--+
                '-3592-4C-'

   .-ESTCAPacity--=--300G-.
>--+----------------------+----------------------------------->
   '-ESTCAPacity--=--size-'

   .-PREFIX--=--ADSM-------------------.
>--+---------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--2----------.  .-COMPression--=--Yes-----.
>--+---------------------------+--+-------------------------+--->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-number-+                     '-No--'
                    '-0------'

>--+-----------------------+----------------------------------->
   +-EXPiration--=--yyyyddd-+
   '-RETention--=--days-----'

   .-PROtection--=--No------------.  .-UNIT--=--3592------.
```

```
>--+-------------------------------+--+--------------------+----><
   '-PROtection--=--+-No--------+-'  '-UNIT--=--unit_name-'
                    +-Yes-------+
                    '-Automatic-'
```

Parameters

device_class_name (Required)
Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

For information about defining a library, see the DEFINE LIBRARY command.

DEVType=3592 (Required)
Specifies the 3592 device type is assigned to the device class.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.
See the following table for the recording formats.

Table 1. Recording formats for 3592

Format	Description
3592	Uncompressed (basic) format
3592C	Compressed format
3592-2	Uncompressed (basic) format, similar to the 3592 format
3592-C	Compressed format, similar to the 3592C format
3592-3	Uncompressed (basic) format, similar to the 3592 format
3592-3C	Compressed format, similar to the 3592C format
3592-4	Uncompressed (basic) format, similar to the 3592 format
3592-4C	Compressed format, similar to the 3592C format
DRIVE	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library containing some drives that support recording formats superior to other drives.
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be different from the listed value.	

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Use the specific format that the drives use. For optimal results, do not mix generations of drives in the same library. If a library contains mixed generations, media problems can result. For example, generation 1 and generation 2 drives cannot read generation 3 media. If possible, upgrade all drives to 3592 generation 3. If you cannot upgrade all drives to 3592 generation 3, you must use a special configuration.

WORM
Specifies whether the drives use WORM (write once, read many) media. This parameter is optional. The default is No. You can specify one of the following values:

Yes
Specifies that the drives use WORM media.

No
Specifies that the drives do not use WORM media.

Tip: The IBM Spectrum Protect™ server does not automatically delete scratch volumes in WORM storage pools after the volumes are emptied by expiration or other processes. To delete these volumes and remove them from WORM storage

pools, you must use the DELETE VOLUME command. IBM Spectrum Protect cannot reuse WORM volumes that were written to by the server and then deleted from a storage pool.

ESTCAPacity
: Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

  You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

  Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

PREFIX
: Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

  If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

  Values that are specified for this parameter must meet the following conditions:

  - The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

    ```
    AB.CD2.E
    ```

  - The qualifiers must be separated by a single period.
  - The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

  An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
: Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. The default value is 60 minutes. Specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait
: Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

  This parameter is optional. The default value is 60. Specify a number, 1 - 9999.

  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is 2.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  You can specify one of the following values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

  number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
Specifies that no new transactions can gain access to the storage pool.

COMPression
Specifies whether file compression is used for this device class. This parameter is optional. The default value is YES. You can specify one of the following values:

Yes
Specifies that the data for each tape volume is compressed.

No
Specifies that the data for each tape volume is not compressed.

EXPiration
Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional. There is no default value.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

PROtection
Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. The default value is NO. You can specify one of the following values:

No
Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Automatic
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the server.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT
Specifies an esoteric unit name to specify a group of tape devices that support 3592 tape. This parameter is optional. The default value is 3592. The unit name can be up to 8 characters.

AIX | Linux

DEFINE DEVCLASS (Define an ECARTRIDGE device class for z/OS media server)

To use a z/OS® media server to access StorageTek drives such as the StorageTek T9840 or T10000, you must define an ECARTRIDGE device class. In the device class definition, specify a library that was defined with the LIBTYPE=ZOSMEDIA parameter.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--------------------------->

>--LIBRary--=--zos_media_library--DEVType--=--ECARTridge-------->

   .-FORMAT--=--DRIVE---------.  .-ESTCAPacity--=--9G---.
>--+------------------------+--+---------------------+------->
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--size-'
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

   .-PREFIX--=--ADSM-----------------.
>--+-----------------------------------+----------------------->
   '-PREFIX--=--+-ADSM--------------+-'
                '-tape_volume_prefix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+--------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

   .-MOUNTLimit--=--2----------.  .-COMPression--=--Yes-----.
>--+-------------------------+--+-----------------------+--->
```

```
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-number-+                     '-No--'
                    '-0------'

>--+-----------------------+---------------------------------->
   +-EXPiration--=--yyyyddd-+
   '-RETention--=--days-----'

   .-PROtection--=--No-----------.  .-UNIT--=--9840------.
>--+---------------------------+--+--------------------+---><
   '-PROtection--=--+-No--------+-'  '-UNIT--=--unit_name-'
                    +-Yes-------+
                    '-Automatic-'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary (Required)

: Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

: For information about defining a library, see the DEFINE LIBRARY command.

DEVType=ECARTridge (Required)
: Specifies that the ECARTRIDGE device type is assigned to the device class. The ECARTRIDGE device type is for StorageTek drives such as the StorageTek T9840 or T10000.

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. See the following table for the recording formats.

Table 1. Recording formats for ECARTRIDGE tapes

Format	Estimated Capacity	Description
DRIVE	-	The server selects the highest format that is supported by the drive on which a volume is mounted. DRIVE is the default value. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library containing some drives that support recording formats superior to other drives.
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

Format	Estimated Capacity	Description
Note: • Some formats use a compression feature of the tape drive hardware. Depending on the effectiveness of compression, the actual capacity might be double or more than the listed value. • T10000A drives can read and write the T10000A format only. T10000B drives can read, but cannot write, the T10000A format. T10000C drives can read, but cannot write, the T10000A and T10000B formats. T10000D drives can read, but cannot write, the T10000A, T10000B, and T10000C formats.		

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional. The default estimated capacity is 9 GB.

You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

PREFIX
Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The default value is ADSM. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. The default value is 60 minutes. Specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait
Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

This parameter is optional. The default value is 60. Specify a number, 1 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. The default is 2.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

You can specify one of the following values:

DRIVES
: Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

number
: Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
: Specifies that no new transactions can gain access to the storage pool.

COMPression
: Specifies whether file compression is used for this device class. This parameter is optional. The default value is YES. You can specify one of the following values:

Yes
: Specifies that the data for each tape volume is compressed.

No
: Specifies that the data for each tape volume is not compressed.

EXPiration
: Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional. There is no default value.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
: Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

PROtection
: Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. The default value is NO. You can specify one of the following values:

No
: Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes
: Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Automatic
: Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the

server.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT
Specifies an esoteric unit name to specify a group of tape devices that support ECARTRIDGE tapes. Use the unit name that represents the subset of drives in the library that are attached to the z/OS system. This parameter is optional. The default value is 9840. The unit name can be up to 8 characters.

Example: Define a device class with the ECARTRIDGE device type

Define a device class named E1 with the ECARTRIDGE device type and with RACF protection active for all tape volumes that are assigned to this device class. All data is compressed for this device class. The device class is for a z/OS media server library named ZOSELIB.

```
define devclass e1 devtype=ecartridge library=zoselib compression=yes
   protection=yes
```

AIX | Linux

DEFINE DEVCLASS (Define a FILE device class for z/OS media server)

To use a z/OS® media server to access storage volumes on magnetic disk devices, you must define a FILE device class. In the device class definition, specify a library that was defined with the LIBTYPE=ZOSMEDIA parameter.

A volume in this device class is a Virtual Storage Access Method (VSAM) linear data set that is accessed by the z/OS media server. SCRATCH volumes can be used with device class and the z/OS media server can dynamically allocate the VSAM LDS. It is not necessary to define volumes for the server to use the device class. If you define volumes, set the high-level qualifier (HLQ) so that SMS recognizes the allocation request by the z/OS media server. If you are using defined volumes, the format volume function is not supported for the server when this device class is used. The z/OS media server uses a FormatWrite feature of DFSMS Media Manager when filling FILE volumes.

You can define volumes for the FILE device class by using the DEFINE VOLUME command. However, the z/OS media server does not allocate space for a defined volume until the volume is opened for its first use.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine DEVclass--device_class_name--DEVType--=--FILE--------->

                              .-MAXCAPacity--=--10G--.
>--LIBRary--=--library_name--+----------------------+---------->
                              '-MAXCAPacity--=--size-'

   .-PRIMARYalloc--=--2600M-.  .-SECONDARYalloc--=--2600M-.
>--+-------------------------+--+-------------------------+----->
   '-PRIMARYalloc--=--size--'  '-SECONDARYalloc--=--size--'

   .-PREFIX--=--ADSM---------------.
>--+-------------------------------+---------------------------->
   '-PREFIX--=--file_volume_prefix-'

   .-MOUNTLimit--=--20-----.
>--+----------------------+---------------------------------><
   '-MOUNTLimit--=--number-'
```

Parameters

DEVType=FILE (Required)
: Specifies that the FILE device type is assigned to the device class.

LIBRary (Required)
: Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The disk storage that is used by this device class is accessed by the z/OS media server and managed by SMS.

  For information about defining a library, see the DEFINE LIBRARY command.

MAXCAPacity
: Specifies the maximum size of file volumes that are defined to a storage pool in this device class. This parameter is optional. The default value is 10 GB (MAXCAPACITY=10G).

  Specify this value as an integer followed by `K` (KB), `M` (MB), `G` (GB), or `T` (TB). The minimum size is 1 MB (MAXCAPACITY=1M). The maximum size is 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc
: Specifies the initial amount of space that is dynamically allocated when a new volume is opened. Enough space must be available to satisfy the primary allocation amount. Storage Management Subsystem (SMS) policy determines whether multiple physical volumes can be used to satisfy the primary allocation request.

  This parameter is optional. Specify this value as an integer followed by `K` (KB), `M` (MB), `G` (GB), or `T` (TB). The minimum size is 100 KB (PRIMARYALLOC=100K). The maximum size is 16384 GB (MAXCAPACITY=16384G). The default size is 2600 MB (PRIMARYALLOC=2600M). All values are rounded to the next higher multiple of 256 KB.

  To avoid wasted space, the dynamic allocation operation uses the smaller of the values that are specified in the two parameters, PRIMARYALLOC and MAXCAPACITY.

  SMS automatic class selection (ACS) routines can affect whether the PRIMARYALLOC and SECONDARYALLOC parameter values are used.

SECONDARYalloc
: Specifies the amount of space by which a file volume is extended when space that is already allocated to the file volume is used up. The data set for a file volume is extended up to the size set by the MAXCAPACITY parameter, then the volume is marked full.

  Because secondary allocation of a linear data set cannot span a physical volume, consider the size of the physical volume when you select a secondary allocation size. For example, physical volumes for a 3390 Model 3 are approximately 2.8 GB. To ensure that each extend request occupies nearly an entire physical volume but not more, use a secondary allocation size that is just less than 2.8 GB. A secondary allocation amount of 2600 MB allots enough space for the VSAM volume data set (VVDS), the volume label, and the volume table of contents (VTOC).

  This parameter is optional. Specify this value as an integer followed by `K` (KB), `M` (MB), `G` (GB), or `T` (TB). The minimum value is 0 KB (SECONDARYALLOC=0K). The default value is 2600 MB. The maximum value is 16384 GB. Except for 0, all values are rounded to the next higher multiple of 256 KB.

  If you specify 0 (SECONDARYALLOC=0), the file volume cannot be extended beyond the primary allocation amount.

SMS automatic class selection (ACS) routines can affect whether the PRIMARYALLOC and SECONDARYALLOC parameter values are used.

If you specify a value for the SECONDARYALLOCATION parameter that is not 0, or if you allow the value to default to 2600M, the SMS DATACLAS associated with the PREFIX identifier (for example, High Level Qualifier) must have the Extended Addressability (EA) attribute specified. Without the EA attribute, the SMS DATACLAS limits the allocation of the VSAM LDS FILE volume to the primary extent. (See the description of the PRIMARYALLOCATION parameter). With the data set limited to primary allocation size, the data set cannot be extended by the z/OS media server, and the volume is marked FULL before the maximum capacity is reached.

Restriction: Ensure that the values that you specify for the PRIMARYALLOC and SECONDARYALLOC parameters are within practical limits for the storage device. The server cannot check whether the values exceed practical device limits, and does not check whether the two values together exceed the current MAXCAPACITY setting.
Tip: To fill volumes when you specify a large value for the MAXCAPACITY parameter, specify large values for the PRIMARYALLOC and SECONDARYALLOC parameters. Use larger MVS™ volume sizes to reduce the chance of extend failure.

PREFIX

Specifies the high-level qualifier of the data set name that is used to allocate scratch volume data sets. For all scratch file volumes created in this device class, the server uses this prefix to create the data set name. This parameter is optional. The default is ADSM. The maximum length of the prefix, including periods, is 32 characters.
Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a file volume data set name using the default prefix is `ADSM.B0000021.BFS`.

If you have a data set naming convention, use a prefix that conforms to your naming conventions. For example, the following value is acceptable: `TSM.SERVER2.VSAMFILE`.

If you are running multiple server instances for either IBM Spectrum Protect™ or Tivoli® Storage Manager for z/OS Media you must use a unique value for the PREFIX parameter for each device class that you define.

MOUNTLimit

Specifies the maximum number of FILE volumes that can be open concurrently for this device class. This parameter is optional. The default value is 20.
If you are using IBM® 3995 devices that emulate 3390 devices, set the value no higher than the number of concurrent input or output streams that are possible on the physical media.

The value that you specify in this parameter is important if there is a significant penalty switching from one volume to another. For example, switching can take place when using IBM 3995 devices to emulate 3390 devices. The value that you specify must be no higher than the number of physical drives available on the device.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

DEFINE DOMAIN (Define a new policy domain)

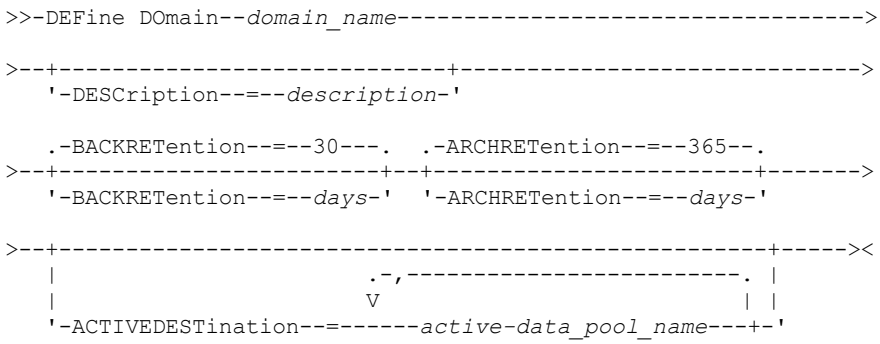
Use this command to define a new policy domain. A policy domain contains policy sets, management classes, and copy groups. A client is assigned to one policy domain. The ACTIVE policy set in the policy domain determines the rules for clients that are assigned to the domain. The rules control the archive, backup, and space management services that are provided for the clients.

You must activate a policy set in the domain before clients assigned to the policy domain can back up, archive, or migrate files.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

domain_name (Required)
: Specifies the name of the policy domain to be defined. The maximum length of this name is 30 characters.

DESCription
: Specifies a description of the policy domain. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

BACKRETention
: Specifies the number of days (from the date the backup versions became inactive) to retain backup versions of files that are no longer on the client file system. This parameter is optional. You can specify an integer from 0 to 9999. The default value is 30. The server uses the backup retention value to manage inactive versions of files when any of the following conditions occur:

  - A file is rebound to a new management class, but the new management class and the default management class do not contain a backup copy group.
  - The management class to which a file is bound no longer exists. The default management class does not contain a backup copy group.
  - The backup copy group is deleted from the management class to which a file is bound. The default management class does not contain a backup copy group.

ARCHRETention
: Specifies the number of days (from the date of archive) to retain archive copies. This parameter is optional. You can specify an integer from 0 to 30000. The default value is 365. The server uses the archive retention value to manage archive copies of files when either of the following conditions occur:

  - The management class to which a file is bound no longer exists. The default management class does not contain an archive copy group.
  - The archive copy group is deleted from the management class to which a file is bound. The default management class does not contain an archive copy group.

ACTIVEDESTination
: This optional parameter specifies the names of active-data pools that store active versions of backup data for nodes that are assigned to the domain. You can specify up to 10 active-data pools for a domain, which is separated by commas. Spaces are not permitted between the names.

  Before the IBM Spectrum Protect™ server writes data to an active-data pool, it verifies that the node owning the data is assigned to a domain that has the active-data pool that is listed in the ACTIVEDESTINATION list. If the server verifies that the node meets this criteria, the data is stored in the active-data pool. If the node does not meet the criteria, then the data is not stored in the active-data pool. If the simultaneous-write function is used to write data to an active-data pool, the server verifies that the node meets the criteria during backup operations by IBM Spectrum Protect backup-archive clients or by application clients by using the IBM Spectrum Protect API. The verification is also performed when active-data is being copied by using the COPY ACTIVEDATA command.

Example: Define a policy domain

Define a policy domain with a name of PROG1 and the description, Programming Group Domain. Specify that archive copies are retained for 90 days when management classes or archive copy groups are deleted and the default management class does not

contain an archive copy group. Also, specify that backup versions are retained for 60 days when management classes or copy groups are deleted and the default management class does not contain a backup copy group.

```
define domain prog1
description="Programming Group Domain"
backretention=60 archretention=90
```

Related commands

Table 1. Commands related to DEFINE DOMAIN

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY DOMAIN	Creates a copy of a policy domain.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE DOMAIN	Deletes a policy domain along with any policy objects in the policy domain.
QUERY DOMAIN	Displays information about policy domains.
UPDATE DOMAIN	Changes the attributes of a policy domain.

DEFINE DRIVE (Define a drive to a library)

Use this command to define a drive. Each drive is assigned to a library, and so the library must be defined before you issue this command.

A path must be defined after you issue the DEFINE DRIVE command to make the drive usable by IBM Spectrum Protect™. For more information, see DEFINE PATH (Define a path). If you are using a SCSI or VTL library type, see PERFORM LIBACTION (Define or delete all drives and paths for a library).

You can define more than one drive for a library by issuing the DEFINE DRIVE command for each drive. Stand-alone drives always require a manual library.

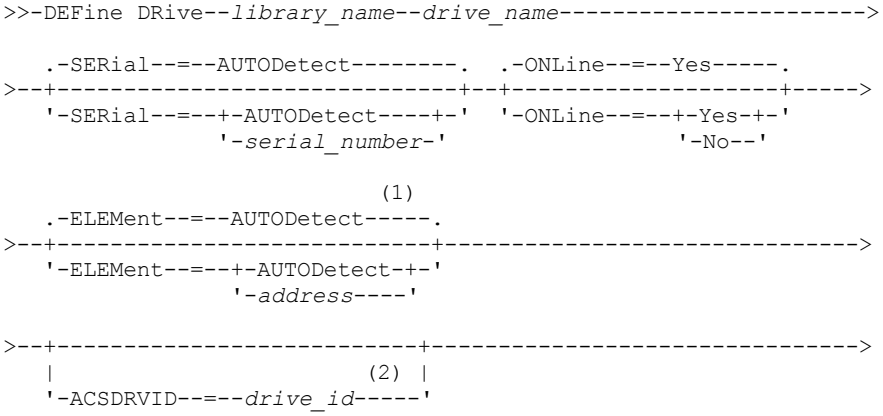
Windows Restriction: Before you issue the DEFINE DRIVE command, for a removable media device such as a Jaz, Zip, or CD drive, you must load the drive with properly formatted and labeled media.
For detailed and current drive support information, see the Supported Devices website for your operating system:

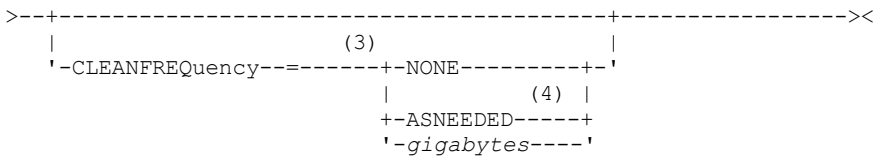
- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax





Notes:

1. The ELEMENT parameter is only necessary for drives in SCSI libraries when the drive type is a network attached SCSI (NAS) drive.
2. ACSDRVID is required for drives in ACSLS libraries. This parameter is not valid for non-ACSLS libraries.
3. The CLEANFREQUENCY parameter is valid only for drives in SCSI libraries.
4. The CLEANFREQUENCY=ASNEEDED parameter value does not work for all tape drives. For more information, see the parameter description.

Parameters

library_name (Required)
: Specifies the name of the library to which the drive is assigned. This parameter is required for all drives, including stand-alone drives. The specified library must have been previously defined by using the DEFINE LIBRARY command.

drive_name (Required)
: Specifies the name that is assigned to the drive. The maximum length of this name is 30 characters.

SERial
: Specifies the serial number for the drive that is being defined. This parameter is optional. The default is AUTODETECT.

  If SERIAL=AUTODETECT, then the serial number reported by the drive when you define the path is used as the serial number.

  If SERIAL=*serial_number*, then the serial number that is entered is used to verify that the path to the drive is correct when you define the path.

  Note: Depending on the capabilities of the device, SERIAL=AUTODETECT might not be supported. In this case, the serial number is reported as blank.

ONLine
: Specifies whether the drive is available for use. This parameter is optional. The default is YES.

  Yes
  : Specifies that the drive is available for use.

  No
  : Specifies that the drive is not available for use.

ELEMent
: Specifies the element address of a drive within a SCSI or virtual tape library (VTL). The server uses the element address to connect the physical location of the drive to the SCSI or VTL address of the drive. The default is AUTODETECT.

  If ELEMENT=AUTODETECT, then the element number is automatically detected by the server when the path to the drive is defined.

  To find the element address for your library configuration, consult the information from the manufacturer.

  Restriction:

  - The ELEMENT parameter is valid only for drives in SCSI libraries or VTLs when the drive type is not a network attached SCSI (NAS) drive.
  - This parameter is not effective when the command is issued from a library client server (that is, when the library type is SHARED).
  - Depending on the capabilities of the library, ELEMENT=AUTODETECT might not be supported. In this case, you must supply the element address.

ACSDRVID
: Specifies the ID of the drive that is being accessed in an ACSLS library. The drive ID is a set of numbers that indicates the physical location of a drive within an ACSLS library. This drive ID must be specified as *a,l,p,d,* where *a* is the ACSID, *l* is the LSM (library storage module), *p* is the panel number, and *d* is the drive ID. The server needs the drive ID to connect the physical location of the drive to the drive's SCSI address. See the StorageTek documentation for details.

Windows Restriction: To use ACSLS functions, the installation of StorageTek Library Attach software is required.

CLEANFREQuency
Specifies how often the server activates drive cleaning. This parameter is optional. For the most complete automation of cleaning for an automated library, you must have a cleaner cartridge that is checked into the library's volume inventory.

If you are using library-based cleaning, NONE is advised when your library type supports this function.

This parameter is not valid for externally managed libraries, such as 3494 libraries or StorageTek libraries that are managed under ACSLS.

Important: There are special considerations if you plan to use server-activated drive cleaning with a SCSI library that provides automatic drive cleaning support in its device hardware.

NONE
Specifies that the server does not track cleaning for this drive. This value can be used for libraries that have their own automatic cleaning.

ASNEEDED
Specifies that the server loads the drive with a checked-in cleaner cartridge only when a drive reports to the device driver that it needs cleaning.

The CLEANFREQUENCY=ASNEEDED parameter value does not work for all tape drives. See the Supported Devices website for your operating system to view detailed drive information. If ASNEEDED is not supported, you can use the gigabytes value for automatic cleaning.

For IBM 3592 and LTO drives, library-based cleaning is advised. If library-based cleaning is not supported, then ASNEEDED must be used. Gigabytes is not recommended.

Restriction: IBM Spectrum Protect does not control the drives that are connected to the NAS file server. If a drive is attached only to a NAS file server (no connection to a storage agent or server), do not specify ASNEEDED for the cleaning frequency.

gigabytes
Specifies, in gigabytes, how much data is processed on the drive before the server loads the drive with a cleaner cartridge. The server resets the gigabytes-processed counter each time it loads a cleaner cartridge in the drive. Important: When CLEANFREQUENCY=gigabyte, drive cleaning can occur before the gigabyte setting is reached, if the drive notifies the device driver that a cleaning is necessary.

Consult the information from the drive manufacturer for cleaning recommendations. If the information gives recommendations for cleaning frequency in terms of hours of use, convert to a gigabytes value by doing the following:

1. Use the bytes-per-second rating for the drive to determine a gigabytes-per-hour value.
2. Multiply the gigabytes-per-hour value by the recommended hours of use between cleanings.
3. Use the result as the cleaning frequency value.

Using the cleaning frequency that is recommended by IBM® for IBM drives ensures that the drives are not overcleaned.

For IBM 3590 drives, specify a gigabyte value for the cleaning frequency to ensure that the drives receive adequate cleaning.

Example: Define a drive to library

Define a drive in a manual library with a library name of LIB01 and a drive name of DRIVE01.

```
define drive lib01 drive01
```

AIX

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=/dev/rmt0
```

Linux

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=/dev/tsmscsi/mt0
```

Windows

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=mt3.0.0.0
```

Example: Define a drive in an ACSLS library

Define a drive in an ACSLS library with a library name of ACSLIB and a drive name of ACSDRV1.

```
define drive acslib acsdrv1 acsdrvid=1,2,3,4
```

AIX

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=/dev/rmt0
```

Linux

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=/dev/tsmscsi/mt0
```

Windows

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=mt3.0.0.0
```

Example: Define a drive in an automated library

Define a drive in an automated library with a library name of AUTO8MMLIB and a drive name of DRIVE01.

```
define drive auto8mmlib drive01 element=82
```

AIX

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/rmt0
```

Linux

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/tsmscsi/mt0
```

Windows

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=mt3.0.0.0
```

Related commands

Table 1. Commands related to DEFINE DRIVE

Command	Description
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DRIVE	Deletes a drive from a library.
DELETE LIBRARY	Deletes a library.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE PATH	Changes the attributes associated with a path.

DEFINE EVENTSERVER (Define a server as the event server)

Use this command to identify a server as the event server.

If you define an event server, one IBM Spectrum Protect™ server can send events to another IBM Spectrum Protect server that will log those events.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine EVENTSERVer--server_name-----------------------------><
```

Parameters

server_name (Required)
: Specifies the name of the event server. The server you specify must have already been defined with the DEFINE SERVER command.

Example: Designate the event server

Designate ASTRO to be the event server.

```
define eventserver astro
```

Related commands

Table 1. Commands related to DEFINE EVENTSERVER

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE EVENTSERVER	Deletes reference to the event server.
DISABLE EVENTS	Disables specific events for receivers.
ENABLE EVENTS	Enables specific events for receivers.
PING SERVER	Tests the connections between servers..
QUERY EVENTSERVER	Displays the name of the event server.
QUERY SERVER	Displays information about servers.

Related information:

Enterprise event logging: logging events to another server

DEFINE GRPMEMBER (Add a server to a server group)

Use this command to add a server as a member of a server group. You can also add one server group to another server group. A server group lets you route commands to multiple servers by specifying only the server group name.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                              .-,-----------.
                              V             |
>>-DEFine GRPMEMber--group_name----member_name-+---------------><
```

Parameters

group_name (Required)
: Specifies the name of the server group to which the member will be added.

member_name (Required)
: Specifies the names of the servers or groups to be added to the group. To specify multiple servers and groups, separate the names with commas and no intervening spaces. The servers or server groups must already be defined to the server.

Example: Define a server to a server group

Define the server SANJOSE to server group CALIFORNIA.

```
define grpmember california sanjose
```

Example: Define a server and a server group to a server group

Define the server TUCSON and the server group CALIFORNIA to server group WEST_COMPLEX.

```
define grpmember west_complex tucson,california
```

Related commands

Table 1. Commands related to DEFINE GRPMEMBER

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.
DEFINE SERVERGROUP	Defines a new server group.
DELETE GRPMEMBER	Deletes a server from a server group.
DELETE SERVERGROUP	Deletes a server group.
MOVE GRPMEMBER	Moves a server group member.
QUERY SERVER	Displays information about servers.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

DEFINE LIBRARY (Define a library)

Use this command to define a library. A library is a collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

A library can be accessed by only one source: an IBM Spectrum Protect™ server or a data mover. However, the drives in a library can be accessed by multiple sources.

The following library types can be defined to the server. Syntax and parameter descriptions are available for each type.

- DEFINE LIBRARY (Define a 349X library)
- DEFINE LIBRARY (Define an ACSLS library)
- DEFINE LIBRARY (Define an External library)
- DEFINE LIBRARY (Define a FILE library)
- DEFINE LIBRARY (Define a manual library)
- DEFINE LIBRARY (Define a SCSI library)
- DEFINE LIBRARY (Define a shared library)
- DEFINE LIBRARY (Define a VTL library)
- AIX Linux DEFINE LIBRARY (Define a ZOSMEDIA library type)

For detailed and current library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Windows

To automatically label tape volumes in SCSI-type libraries, use the AUTOLABEL parameter on the DEFINE LIBRARY and UPDATE LIBRARY commands. Using this parameter eliminates the need to pre-label a set of tapes. It is also more efficient than using the LABEL LIBVOLUME command, which requires you to mount volumes separately. If you use the AUTOLABEL parameter, you must check in tapes by specifying CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

A label cannot include embedded blanks or periods and must be valid when used as a file name on the media.

You must label CD-ROM, Zip, or Jaz volumes with the device utilities from the manufacturer or the Windows utilities because IBM Spectrum Protect does not provide utilities to format or label these media types. The operating system utilities include the Disk Administrator program (a graphical user interface) and the label command.

Related commands

Table 1. Commands related to DEFINE LIBRARY

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE PATH	Defines a path from a source to a destination.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE DRIVE	Deletes a drive from a library.
DELETE LIBRARY	Deletes a library.
DELETE PATH	Deletes a path from a source to a destination.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE LIBRARY	Changes the attributes of a library.
UPDATE LIBVOLUME	Changes the status of a storage volume.
UPDATE PATH	Changes the attributes associated with a path.

DEFINE LIBRARY (Define a 349X library)

Use this syntax to define a 349X library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType--=--349X--------------->

   .-SHAREd--=--No------.  .-RESETDrives--=--No----------.
```

```
>--+--------------------+--+----------------------------+------>
   '-SHAREd--=--+-Yes-+-'  |                          (1) |
                '-No--'    '-RESETDrives--=--+-Yes-+-----'
                                             '-No--'

   .-AUTOLabel--=--Yes-----------.
>--+-----------------------------+----------------------------->
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

   .-SCRATCHCATegory--=--301----.
>--+----------------------------+----------------------------->
   '-SCRATCHCATegory--=--number-'

   .-PRIVATECATegory--=--300----.
>--+----------------------------+----------------------------->
   '-PRIVATECATegory--=--number-'

>--+-------------------------------+-------------------------><
   '-WORMSCRatchcategory--=--number-'
```

Notes:

1. The default value of the RESETDRIVES parameter is conditional. If the SHARED parameter is set to NO, the value of the RESETDRIVES parameter is NO. If the SHARED parameter is set to YES, the value of the RESETDRIVES parameter is YES.

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=349X (Required)

: AIX Linux Specifies that the library is an IBM 3494 or 3495 Tape Library Dataserver.

: Windows Specifies that the library is an IBM 3494 Tape Library Dataserver or an IBM Tape System Library Manager emulating a 3494 Tape Library Dataserver.

: Restriction: IBM 3494 libraries support only one unique device type at a time.

SHAREd
: Specifies whether this library is shared with other servers in a storage area network (SAN). This parameter is required when you define a library to the library manager.

: YES
: Specifies that this library can be shared with other servers. When you specify YES, the library manager server mounts volumes as requested by other servers and tracks drive and volume allocation to other servers.

: NO
: Specifies that this library cannot be shared with other servers. SHARED=NO is required if the library is controlled by passing commands through a NAS file server.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is YES.

: To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

: Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

: No
: Specifies that the server does not attempt to label any volumes.

: Yes
: Specifies that the server labels only unlabeled volumes.

: OVERWRITE
: Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels only if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

SCRATCHCATegory

Specifies the category number to be used for scratch volumes in the library. This parameter is optional. The default value is 301 (becomes X'12D' on the IBM 3494 since it uses hexadecimal values). You can specify a number from 1 to 65279. This number must be unique. It cannot be shared with other applications or defined libraries, and it must be different from the other category numbers in this library.

PRIVATECATegory

Specifies the category number for private volumes that must be mounted by name. This parameter is optional. The default value is 300 (this value becomes X'12C' on the IBM 3494 because it uses hexadecimal values). You can specify a number from 1 to 65279. This number must be unique. It cannot be shared with other applications or defined libraries, and it must be different from the other category numbers in this library.

WORMSCRatchcategory

Specifies the category number to be used for WORM scratch volumes in the library. This parameter is required if you use WORM volumes. You can specify a number from 1 to 65279. This number must be unique. It cannot be shared with other applications or defined libraries, and it must be different from the other category numbers in this library. This parameter is only valid when 3592 WORM volumes are used.

Restriction: If the WORMSCRATCHCATEGORY is not defined and the WORM parameter is set to YES for the device class, the mount operation fails with an error message.

RESETDrives

Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established. If, for example, a storage agent becomes unavailable but is still holding the path to a drive, persistent reserve allows the server to break the storage agent's reservation and access the drive.

AIX Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

The following table describes the three possible configurations for drives that are attached to NAS devices.

Table 1. Configurations for drives that are attached to NAS devices.

Library device configuration	**The behavior for persistent reserve**
The library device is attached to the IBM Spectrum Protect server, and the tape drives are shared by the server and the NAS device.	Drive reservation preemption is supported when the NAS device supports persistent reserve and it is enabled. For more information about setting persistent reserve, see the documentation for your NAS device.
The library device is attached to the IBM Spectrum Protect server and the tape drives are accessed only from the NAS device.	Drive reservation preemption is not supported. If you enable persistent reserve on the NAS device for these drives and a reservation is set by the NAS device but never cleared, you must use another method to clear the reservation.

AIX Windows

Yes

Specifies that drive preemption through persistent reserve or target reset are used. YES is the default for a library that is defined with SHARED=YES.

No

Specifies that drive preemption through persistent reserve or target reset are not used. NO is the default for a library that is defined with SHARED=NO. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes

Specifies that drive preemption through persistent reserve is used. YES is the default for a library that is defined with SHARED=YES.

No

Specifies that drive preemption through persistent reserve is not used. NO is the default for a library that is defined with SHARED=NO.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

Example: Define a 3494 library

Define a library named `my3494` with a scratch category number of 550, a private category number of 600, and a WORM scratch category number of 400®

```
define library my3494 libtype=349x scratchcategory=550
privatecategory=600 wormscratchcategory=400
```

DEFINE LIBRARY (Define an ACSLS library)

Use this syntax to define an ACSLS library.

Privilege class

Windows To use ACSLS functions, the installation of StorageTek Library Attach software is required.

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType--=--ACSLS-------------->

   .-SHAREd--=--No------.  .-RESETDrives--=--No----------.
>--+--------------------+--+---------------------------+------>
   '-SHAREd--=--+-Yes-+-'  |                       (1) |
                '-No--'    '-RESETDrives--=--+-Yes-+-----'
                                             '-No--'

   .-AUTOLabel--=--Yes-----------.
>--+----------------------------+--ACSID--=--number----------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Notes:

1. The default value of the RESETDRIVES parameter is conditional. If the SHARED parameter is set to NO, the value of the RESETDRIVES parameter is NO. If the SHARED parameter is set to YES, the value of the RESETDRIVES parameter is YES.

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=ACSLS (Required)
: Specifies that the library is a StorageTek library that is controlled by StorageTek Automated Cartridge System Library Software (ACSLS).

SHAREd
: Specifies whether this library is shared with other servers in a storage area network (SAN). This parameter is required when you define a library to the library manager.

  YES
  : Specifies that this library can be shared with other servers. When you specify YES, the library manager server mounts volumes as requested by other servers and tracks drive and volume allocation to other servers.

  NO
  : Specifies that this library cannot be shared with other servers. SHARED=NO is required if the library is controlled by passing commands through a NAS file server.

RESETDrives

Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established. If, for example, a storage agent becomes unavailable but is still holding the path to a drive, persistent reserve allows the server to break the storage agent's reservation and access the drive.

AIX Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

The following table describes the three possible configurations for drives that are attached to NAS devices.

Table 1. Configurations for drives that are attached to NAS devices.

Library device configuration	The behavior for persistent reserve
The library device is attached to the IBM Spectrum Protect server, and the tape drives are shared by the server and the NAS device.	Drive reservation preemption is supported when the NAS device supports persistent reserve and it is enabled. For more information about setting persistent reserve, see the documentation for your NAS device.
The library device is attached to the IBM Spectrum Protect server and the tape drives are accessed only from the NAS device.	Drive reservation preemption is not supported. If you enable persistent reserve on the NAS device for these drives and a reservation is set by the NAS device but never cleared, you must use another method to clear the reservation.

AIX Windows

Yes

Specifies that drive preemption through persistent reserve or target reset are used. YES is the default for a library that is defined with SHARED=YES.

No

Specifies that drive preemption through persistent reserve or target reset are not used. NO is the default for a library that is defined with SHARED=NO. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes

Specifies that drive preemption through persistent reserve is used. YES is the default for a library that is defined with SHARED=YES.

No

Specifies that drive preemption through persistent reserve is not used. NO is the default for a library that is defined with SHARED=NO.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

AUTOLabel

Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is YES.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

No

Specifies that the server does not attempt to label any volumes.

Yes

Specifies that the server labels only unlabeled volumes.

OVERWRITE
Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

ACSID (Required)
Specifies the number of this StorageTek library that is assigned by the ACSSA (Automatic Cartridge System System Administrator). This number can be from 0 to 126. Issue QUERY ACS on your system to get the number for your library ID. This parameter is required.

For more information, see your StorageTek documentation.

Example: Define a shared ACSLS library

Define a library named ACSLIB with the library type of ACSLS and an ACSID of 1.

```
define library acslib libtype=acsls acsid=1 shared=yes
```

DEFINE LIBRARY (Define an External library)

Use this syntax to define an External library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType--=--EXTernal----------->

   .-AUTOLabel--=--Yes----------.
>--+----------------------------+----------------------------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameters

library_name (Required)
Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=EXTernal (Required)
Specifies that the library is managed by an external media management system. This library type does not support drive definitions with the DEFINE DRIVE command. Rather, the external media management system identifies the appropriate drive for media access operations.

AIX Windows In an IBM Spectrum Protect™ for Storage Area Networks environment, this parameter specifies that StorageTek Automated Cartridge System Library Software (ACSLS) or Library Station software controls the library. Software, such as Gresham EDT-DistribuTAPE, allows multiple servers to share the library. The drives in this library are not defined to IBM Spectrum Protect. ACSLS identifies the drive for media operations.

AUTOLabel
Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is YES.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
Specifies that the server does not attempt to label any volumes.
Yes
Specifies that the server labels only unlabeled volumes.
OVERWRITE
Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

Example: Define an external library for a SAN configuration

For an IBM Spectrum Protect for Storage Area Networks configuration, define a library named EXTLIB with the library type of EXTERNAL. If you are using Gresham Enterprise DistribuTAPE, the external library manager executable file is in the following directory:

- AIX /usr/lpp/dtelm/bin/elm
- Linux /opt/OMIdtelm/bin/elm
- Windows c:\program files\GES\EDT\bin\elm.exe

If you are using the IBM® Tape System Library Manager, the external library manager executable file can be found in the following directory:

- AIX Linux /opt/IBM/TSLM/client/tsm/elm
- Windows ...\IBM\rmm\client\tsm\elm.exe

For more information, see the *IBM Tape System Library Manager User's Guide* at http://www-01.ibm.com/support/docview.wss?uid=pub1ga32220802.

1. Define the library:

```
define library extlib libtype=external
```

2. Define the path:

AIX

```
define path server1 extlib srctype=server desttype=library
  externalmanager="/usr/lpp/dtelm/bin/elm"
```

Linux

```
define path server1 extlib srctype=server desttype=library
  externalmanager="/opt/OMIdtelm/bin/elm"
```

Windows

```
define path server1 extlib srctype=server desttype=library
  externalmanager="c:\program files\GES\EDT\bin\elm.exe"
```

DEFINE LIBRARY (Define a FILE library)

Use this syntax to define a FILE library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType--=--FILE---------------><

   .-SHAREd--=--No------.
>--+--------------------+-------------------------------------><
   '-SHAREd--=--+-Yes-+-'
                '-No--'
```

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=FILE (Required)
: Specifies that a pseudo-library is created for sequential file volumes. When you issue the DEFINE DEVCLASS command with DEVTYPE=FILE and SHARED=YES parameters, this occurs automatically. FILE libraries are necessary only when sharing sequential file volumes between the server and one or more storage agents. The use of FILE libraries requires

library sharing. Shared FILE libraries are supported for use in LAN-free backup configurations only. You cannot use a shared FILE library in an environment in which a library manager is used to manage library clients.

SHAREd
: Specifies whether this library is shared with other IBM Spectrum Protect™ servers in a storage area network (SAN). This parameter is required when you define a library to the library manager.

  YES
  : Specifies that this library can be shared with other servers. When you specify YES, the library manager server mounts volumes as requested by other servers and tracks drive and volume allocation to other servers.

  NO
  : Specifies that this library cannot be shared with other servers. SHARED=NO is required if the library is controlled by passing commands through a NAS file server.

Example: Define a shared FILE library

Define a file library with shared=yes.

```
define library file1 libtype=file shared=yes
```

DEFINE LIBRARY (Define a manual library)

Use this syntax to define a manual library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType---=--MANUAL------------>

   .-RESETDrives---=---Yes-----.
>--+-------------------------+---------------------------------->
   '-RESETDrives---=---+-Yes-+-'
                       '-No--'

   .-AUTOLabel---=---Yes-----------.
>--+-----------------------------+----------------------------><
   '-AUTOLabel---=---+-No--------+-'
                     +-Yes-------+
                     '-OVERWRITE-'
```

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=MANUAL (Required)
: Specifies that the library is not automated. When volumes must be mounted on drives in this type of library, messages are sent to operators. This type of library is used with stand-alone drives.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is YES.

  To use this option, you need to check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

  No
  : Specifies that the server does not attempt to label any volumes.

  Yes
  : Specifies that the server only labels unlabeled volumes.

  OVERWRITE
  : Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

RESETDrives
Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established. If, for example, a storage agent becomes unavailable but is still holding the path to a drive, persistent reserve allows the server to break the storage agent's reservation and access the drive.

AIX | Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

AIX | Windows

Yes
Specifies that drive preemption through persistent reserve or target reset are used. YES is the default for a library that is defined with SHARED=YES.

No
Specifies that drive preemption through persistent reserve or target reset are not used. NO is the default for a library that is defined with SHARED=NO. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
Specifies that drive preemption through persistent reserve is used. YES is the default for a library that is defined with SHARED=YES.

No
Specifies that drive preemption through persistent reserve is not used. NO is the default for a library that is defined with SHARED=NO.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

Example: Define a manual library

Define a library named `MANUALMOUNT` with the library type of MANUAL.

```
define library manualmount libtype=manual
```

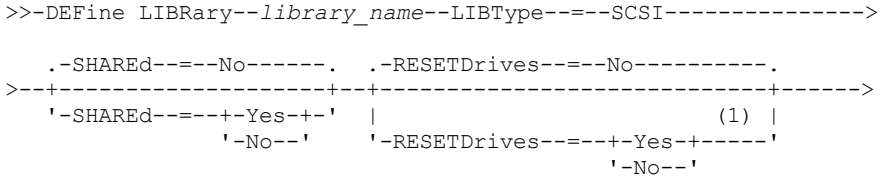
DEFINE LIBRARY (Define a SCSI library)

Use this syntax to define a SCSI library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



```
   .-AUTOLabel--=--No------------.
>--+-----------------------------+------------------------------>
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

   .-RELABELSCRatch--=--No------.
>--+-----------------------------+------------------------------>
   '-RELABELSCRatch--=--+-No--+-'
                        '-Yes-'

   .-SERial--=--AUTODetect--------.
>--+-----------------------------+----------------------------><
   '-SERial--=--+-AUTODetect----+-'
                '-serial_number-'
```

Notes:

1. The default value of the RESETDRIVES parameter is conditional. If the SHARED parameter is set to NO, the value of the RESETDRIVES parameter is NO. If the SHARED parameter is set to YES, the value of the RESETDRIVES parameter is YES.

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=SCSI (Required)
: Specifies that the library has a SCSI-controlled media changer device. To mount volumes on drives in this type of library, the server uses the media changer device.

SHAREd
: Specifies whether this library is shared with other servers in a storage area network (SAN). This parameter is required when you define a library to the library manager.

  YES
  : Specifies that this library can be shared with other servers. When you specify YES, the library manager server mounts volumes as requested by other servers and tracks drive and volume allocation to other servers.

  NO
  : Specifies that this library cannot be shared with other servers. SHARED=NO is required if the library is controlled by passing commands through a NAS file server.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is NO.

  To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

  Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

  No
  : Specifies that the server does not attempt to label any volumes.

  Yes
  : Specifies that the server labels only unlabeled volumes.

  OVERWRITE
  : Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

RELABELSCRatch
: Specifies whether the server relabels volumes that were deleted and returned to scratch. When this parameter is set to YES, a LABEL LIBVOLUME operation is started and the existing volume label is overwritten. This parameter is optional and intended for use with a Virtual Tape Library (VTL).

  If you have both virtual and real volumes in your VTL, both types are relabeled when this parameter is enabled. If the VTL includes real volumes, specifying this option might impact performance.

  Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

No
: Specifies that the server does not relabel volumes that are deleted and returned to scratch.

Yes
: Specifies that the server relabels volumes that are deleted and returned to scratch.

RESETDrives
: Specifies whether the server preempts a drive reservation if the drive is already reserved by persistent reserve when the server tries to access the drive. For example, a storage agent becomes unavailable, but the agent still holds the drive that is reserved through persistent reserve. With persistent reserve, the server can break a drive reservation and access the drive.

AIX Windows If the drive is reserved by a SCSI-2 reserve, (and not by persistent reserve), the server uses a LUN reset to break the drive reservation to access the target device.

Linux LUN resets are not supported by the Linux operating system. If a drive is reserved by a SCSI-2 reserve, (and not by persistent reserve), the server is unable to break the reservation to access the drive. In this case, you can break the reservation by power cycling the device.

For network-attached storage (NAS) devices, reservation is controlled by the NAS file server. IBM Spectrum Protect™ does not control NAS devices and the RESETDrives parameter is not relevant for NAS devices.

Support for persistent reserve has the following limitations:

- If you are using the IBM Spectrum Protect device driver, persistent reserve is supported only on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. For information about driver configuration, see the *IBM Tape Device Drivers Installation and User's Guide*.
- If you are using a virtual tape library that is emulating a supported drive, persistent reserve might not be supported.
- A library manager is not able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reserve.

AIX Windows

Yes
: Specifies that drive preemption through persistent reserve or target reset is used. YES is the default for a library that is defined with SHARED=YES.

No
: Specifies that drive preemption through persistent reserve or target reset is not used. NO is the default for a library that is defined with SHARED=NO. The RESETDrives parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
: Specifies that drive preemption through persistent reserve is used. YES is the default for a library that is defined with SHARED=YES.

No
: Specifies that drive preemption through persistent reserve is not used. NO is the default for a library that is defined with SHARED=NO.

SERial
: Specifies the serial number for the library that is being defined. This parameter is optional. The default is AUTODETECT.

If SERIAL=AUTODETECT, then when you define the path to the library, the serial number reported by the library is used as the serial number.

If SERIAL=*serial_number*, then the number you entered is compared to the number detected by the server.

Attention: Depending on the capabilities of the device, SERIAL=AUTODETECT might not be supported. In this case, the serial number is reported as blank.

Example: Define a SCSI library

Define a library that is named SCSILIB with a library type of SCSI.

```
define library scsilib libtype=scsi
```

The library requires a path. The device name for the library is:

- AIX `/dev/lb0`
- Linux `/dev/tsmscsi/lb0`
- Windows `lb3.0.0.0`

Define the path:

AIX

```
define path server1 scsilib srctype=server desttype=library
   device=/dev/lb0
```

Linux

```
define path server1 scsilib srctype=server desttype=library
   device=/dev/tsmscsi/lb0
```

Windows

```
define path server1 scsilib srctype=server desttype=library
   device=lb3.0.0.0
```

DEFINE LIBRARY (Define a shared library)

Use this syntax to define a shared library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType--=--SHAREd------------>

>--PRIMarylibmanager--=--server_name--------------------------><
```

Parameters

library_name (Required)
: Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=SHAREd (Required)
: Specifies that the library is shared with another IBM Spectrum Protect™ server over a storage area network (SAN) or a dual SCSI connection to library drives.
: Important: Specify this library type when you define the library on a library client.

PRIMarylibmanager
: Specifies the name of the IBM Spectrum Protect server that is responsible for controlling access to library resources. You must define this server with the DEFINE SERVER command before you can use it as a library manager. This parameter is required and valid only if LIBTYPE=SHARED.

Example: Define a shared library

In a SAN, define a library named `SHAREDTSM` to a library client server named LIBMGR1

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

DEFINE LIBRARY (Define a VTL library)

Use this syntax to define a library that has a SCSI-controlled media changer device that is represented by a virtual tape library (VTL).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Notes:

1. The default value of the RESETDRIVES parameter is conditional. If the SHARED parameter is set to NO, the value of the RESETDRIVES parameter is NO. If the SHARED parameter is set to YES, the value of the RESETDRIVES parameter is YES.

Parameters

library_name (Required)
Specifies the name of the library to be defined. The maximum length of this name is 30 characters.

LIBType=VTL (Required)
Specifies that the library has a SCSI-controlled media changer device that is represented by a virtual tape library. To mount volumes in drives in this type of library, the server uses the media changer device.

If you are defining a VTL library, your environment must not include any mixed-media and paths must be defined between all drives in the library and all defined servers, including storage agents, that use the library. If either of these characteristics are not true, the overall performance can degrade to the same levels as the SCSI library type; especially during times of high stress.

SHAREd
Specifies whether this library is shared with other servers in a storage area network (SAN). This parameter is required when you define a library to the library manager.

YES
Specifies that this library can be shared with other servers. When you specify YES, the library manager server mounts volumes as requested by other servers and tracks drive and volume allocation to other servers.

NO
Specifies that this library cannot be shared with other servers. SHARED=NO is required if the library is controlled by passing commands through a NAS file server.

RESETDrives
Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established. If, for example, a storage agent becomes unavailable but is still holding the path to a drive, persistent reserve allows the server to break the storage agent's reservation and access the drive.

AIX | Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

AIX | Windows

Yes
: Specifies that drive preemption through persistent reserve or target reset are used. YES is the default for a library that is defined with SHARED=YES.

No
: Specifies that drive preemption through persistent reserve or target reset are not used. NO is the default for a library that is defined with SHARED=NO. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
: Specifies that drive preemption through persistent reserve is used. YES is the default for a library that is defined with SHARED=YES.

No
: Specifies that drive preemption through persistent reserve is not used. NO is the default for a library that is defined with SHARED=NO.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional. The default is NO.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

No
: Specifies that the server does not attempt to label any volumes.

Yes
: Specifies that the server labels only unlabeled volumes.

OVERWRITE
: Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

RELABELSCRatch
: Specifies whether the server relabels volumes that were deleted and returned to scratch. When this parameter is set to YES, a LABEL LIBVOLUME operation is started and the existing volume label is overwritten.

If you have both virtual and real volumes in your VTL, both types are relabeled when this parameter is enabled. If the VTL includes real volumes, specifying this option might impact performance.

Restriction: If you are defining a library that has drives that are attached to a network-attached storage (NAS) device, you must use the LABEL LIBVOLUME command to label the volumes for this library.

Yes
: Specifies that the server relabels volumes that are deleted and returned to scratch. YES is the default.

No
: Specifies that the server does not relabel volumes that are deleted and returned to scratch.

SERial
: Specifies the serial number for the library that is being defined. This parameter is optional. The default is AUTODETECT.

If SERIAL=AUTODETECT, then when you define the path to the library, the serial number reported by the library is used as the serial number.

If SERIAL=*serial_number*, then the number you entered is compared to the number detected by the server.

Attention: Depending on the capabilities of the device, SERIAL=AUTODETECT might not be supported. In this case, the serial number is reported as blank.

Example: Define a VTL library

Define a library named VTLLIB with a library type of VTL.

```
define library vtllib libtype=vtl
```

The library requires a path. The device name for the library is:

- AIX /dev/lb0
- Linux /dev/tsmscsi/lb0
- Windows lb3.0.0.0

Define the path:

AIX

```
define path server1 vtllib srctype=server desttype=library
   device=/dev/lb0
```

Linux

```
define path server1 vtllib srctype=server desttype=library
   device=/dev/tsmscsi/lb0
```

Windows

```
define path server1 vtllib srctype=server desttype=library
   device=lb3.0.0.0
```

AIX | Linux

DEFINE LIBRARY (Define a ZOSMEDIA library type)

Use this syntax to define a library that represents a TAPE or FILE storage resource that is maintained by Tivoli® Storage Manager for z/OS® Media.

Define a library of type ZOSMEDIA when you want the library to be exclusively managed by Tivoli Storage Manager for z/OS Media. The library appears to the IBM Spectrum Protect™ server as a logical storage device that does not require DRIVE definitions. A PATH definition is required for the server and any storage agents that need access to the ZOSMEDIA library resource.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine LIBRary--library_name--LIBType---=--ZOSMEDIA----------><
```

Parameters

library_name (Required)
: Specifies the name of the library to be defined.

LIBType=ZOSMEDIA (Required)
: Specifies that the library type is the ZOSMEDIA which represents a TAPE or FILE storage resource that is maintained by Tivoli Storage Manager for z/OS Media.

Example: Configure a ZOSMEDIA library

The following example shows the steps needed to define and configure a zosmedia library. The configuration includes these components:

- A server named sahara
- A library defined as type zosmedia named zebra
- A z/OS media server named oasis
- A storage agent named mirage

Define a library named ZEBRA with a library type of ZOSMEDIA:

```
define library zebra libtype=zosmedia
```

Define the z/OS media server:

```
define server oasis serverpassword=sanddune
hladdress=9.289.19.67 lladdress=1777
```

The server requires a path to the library resource managed by Tivoli Storage Manager for z/OS Media:

```
define path sahara zebra srctype=server
desttype=library zosmediaserver=oasis
```

The storage agent requires a path to the library resource managed by Tivoli Storage Manager for z/OS Media:

```
define path mirage zebra srctype=server
desttype=library zosmediaserver=oasis
```

DEFINE MACHINE (Define machine information for disaster recovery)

Use this command to save disaster recovery information for a server or client node machine. This information will be included in the plan file to help you recover your machines.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine MACHine--machine_name---------------------------------->

>--+-----------------------------+--+-----------------------+--->
   '-DESCription--=--description-'  '-BUilding--=--building-'

>--+-----------------+--+--------------+----------------------->
   '-FLoor--=--floor-'  '-ROom--=--room-'

   .-PRIority--=--50---------.  .-ADSMServer--=--No------.
>--+-------------------------+--+----------------------+-----><
   '-PRIority--=----number---'  '-ADSMServer--=--+-No--+-'
                                                 '-Yes-'
```

Parameters

machine_name (Required)
: Specifies the machine name. The name can be up to 64 characters.

DESCription
: Specifies a machine description. This parameter is optional. The text can be up to 255 characters. Enclose the text in quotation marks if it contains any blank characters.

BUilding
: Specifies the building that this machine is in. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters.

FLoor
: Specifies the floor that this machine is on. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters.

ROom
: Specifies the room that this machine is in. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters.

PRIority
: Specifies the restore priority for the machine an integer from 1 to 99. The highest priority is 1. This parameter is optional. The default is 50.

ADSMServer
: Specifies whether the machine is an IBM Spectrum Protect™ server. Only one machine can be defined as an IBM Spectrum Protect server. This parameter is optional. The default is NO. Possible values are:

  No
  : This machine is not an IBM Spectrum Protect server.

  Yes
  : This machine is an IBM Spectrum Protect server.

Example: Define a machine's disaster recovery information

Define a machine named DISTRICT5, and specify a location, a floor, and a room name. This machine contains critical data and has the highest priority.

```
define machine district5 building=101 floor=27
room=datafacilities priority=1
```

Related commands

Table 1. Commands related to DEFINE MACHINE

Command	Description
DEFINE MACHNODEASSOCIATION	Associates an IBM Spectrum Protect node with a machine.
DEFINE RECMEDMACHASSOCIATION	Associates recovery media with a machine.
DELETE MACHINE	Deletes a machine.
INSERT MACHINE	Inserts machine characteristics or recovery instructions into the IBM Spectrum Protect database.
QUERY MACHINE	Displays information about machines.
UPDATE MACHINE	Changes the information for a machine.

DEFINE MACHNODEASSOCIATION (Associate a node with a machine)

Use this command to associate client nodes with a machine. During disaster recovery, you can use this information to identify the client nodes that resided on destroyed machines.

The machine must be defined and the nodes registered to IBM Spectrum Protect™.

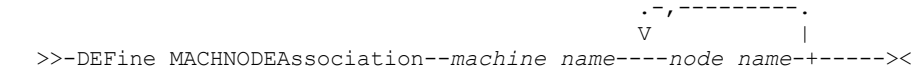
To retrieve the information, issue the QUERY MACHINE command. This information will be included in the plan file to help you recover the client machines.

A node remains associated with a machine unless the node, the machine, or the association itself is deleted.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

machine_name (Required)

Specifies the machine name.

node_name (Required)

Specifies the node names. A node can only be associated with one machine. To specify multiple nodes, separate the names with commas and no intervening spaces. You can use wildcard characters to specify a name.

Example: Associate a node with a machine

Associate the node named ACCOUNTSPAYABLE with the machine named DISTRICT5.

```
define machnodeassociation district5 accountspayable
```

Related commands

Table 1. Commands related to DEFINE MACHNODEASSOCIATION

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
DELETE MACHINE	Deletes a machine.
DELETE MACHNODEASSOCIATION	Deletes association between a machine and node.
QUERY MACHINE	Displays information about machines.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.

DEFINE MGMTCLASS (Define a management class)

Use this command to define a new management class in a policy set. To allow clients to use the new management class, you must activate the policy set that contains the new class.

You can define one or more management classes for each policy set in a policy domain. A management class can contain a backup copy group, an archive copy group, or both. The user of a client node can select any management class in the active policy set or use the default management class.

Attention: The DEFINE MGMTCLASS command fails if a copy storage pool is specified as the destination for files that were migrated by an IBM Spectrum Protect™ for Space Management client.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the management class belongs.

Syntax

```
>>-DEFine MGmtclass--domain_name--policy_set_name--class_name--->

   .-SPACEMGTECHnique--=--NONE----------.
>--+-----------------------------------+---------------------->
   '-SPACEMGTECHnique--=--+-AUTOmatic-+-'
                          +-SELective-+
                          '-NONE------'

   .-AUTOMIGNOnuse--=--0----.
>--+-----------------------+---------------------------------->
   '-AUTOMIGNOnuse--=--days-'

   .-MIGREQUIRESBkup--=--Yes-----.
>--+-----------------------------+---------------------------->
   '-MIGREQUIRESBkup--=--+-Yes-+-'
                         '-No--'
```

```
   .-MIGDESTination--=--SPACEMGPOOL-.
>--+--------------------------------+--------------------------->
   '-MIGDESTination--=--pool_name---'

>--+----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the management class belongs.

policy_set_name (Required)
: Specifies the policy set to which the management class belongs. You cannot define a management class to the ACTIVE policy set.

class_name (Required)
: Specifies the name of the new management class. The maximum length of this name is 30 characters. You cannot use either *default* or *grace_period* as a class name.

SPACEMGTECHnique
: Specifies whether a file that is using this management class is eligible for migration. This parameter is optional. The default is NONE. This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients. Possible values are:

  AUTOmatic
  : Specifies that the file is eligible for both automatic migration and selective migration.

  SELective
  : Specifies that the file is eligible for selective migration only.

  NONE
  : Specifies that the file is not eligible for migration.

AUTOMIGNOnuse
: Specifies the number of days that must elapse since a file was last accessed before it is eligible for automatic migration. This parameter is optional. The default value is 0. If SPACEMGTECHNIQUE is not AUTOMATIC, the server ignores this attribute. You can specify an integer in the range 0 - 9999.

  This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients.

MIGREQUIRESBkup
: Specifies whether a backup version of a file must exist before a file can be migrated. This parameter is optional. The default is YES. This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients. Possible values are:

  Yes
  : Specifies that a backup version must exist.

  No
  : Specifies that a backup version is optional.

MIGDESTination
: Specifies the primary storage pool where the server initially stores files that are migrated by IBM Spectrum Protect for Space Management clients. This parameter is effective only for IBM Spectrum Protect for Space Management clients, and is not effective for backup-archive clients or application clients. The default is SPACEMGPOOL.
  Your choice for the destination might depend on factors such as the following:

  - The number of client nodes that are migrated to the storage pool. When many user files are stored in the same storage pool, volume contention can occur as users try to migrate files to or recall files from the storage pool.
  - How quickly the files must be recalled. If you need immediate access to migrated versions, you can specify a disk storage pool as the destination.

  The command fails if you specify a copy storage pool or an active-data pool as the destination.

DESCription
: Specifies a description of the management class. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Example: Define a management class for a specific policy set and policy domain

Define a management class that is called MCLASS1 for policy set SUMMER in the PROG1 policy domain. For IBM Spectrum Protect for Space Management clients, allow both automatic and selective migration, and store migrated files in the SMPOOL storage pool. Add the description, "Technical Support Mgmt Class."

```
define mgmtclass prog1 summer mclass1
spacemgtechnique=automatic migdestination=smpool
description="technical support mgmt class"
```

Related commands

Table 1. Commands related to DEFINE MGMTCLASS

Command	Description
ASSIGN DEFMGMTCLASS	Assigns a management class as the default for a specified policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.
QUERY POLICYSET	Displays information about policy sets.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE MGMTCLASS	Changes the attributes of a management class.

DEFINE NODEGROUP (Define a node group)

Use this command to define a node group. A *node group* is a group of client nodes that are acted upon as if they were a single entity. A node can be a member of one or more node groups.

Privilege class

To issue this command, you must have system or unrestricted policy privilege.

Syntax

```
>>-DEFine NODEGroup--group_name---------------------------------->

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

group_name
: Specifies the name of the node group that you want to create. The maximum length of the name is 64 characters. The specified name may not be the same as any existing client node name.

DESCription
: Specifies a description of the node group. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Example: Define a node group

Define a node group named `group1`.

```
define nodegroup group1
```

Related commands

Table 1. Commands related to DEFINE NODEGROUP

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

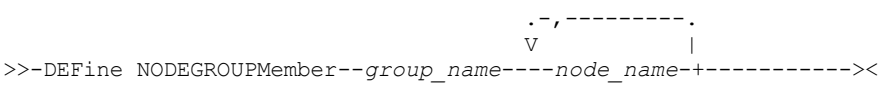
DEFINE NODEGROUPMEMBER (Define node group member)

Use this command to add a client node to a node group. A *node group* is a group of client nodes that are acted upon as if they were a single entity.

Privilege class

To issue this command you must have system or unrestricted policy privilege.

Syntax



Parameters

group_name
: Specifies the name of the node group to which you want to add a client node.

node_name
: Specifies the name of the client node that you want to add to the node group. You can specify one or more names. Separate multiple names with commas; do not use intervening spaces. You can also use wildcard characters when specifying multiple names.

Example: Define node group members

Define two members, `node1` and `node2`, to a node group, `group1`.

```
define nodegroupmember group1 node1,node2
```

Related commands

Table 1. Commands related to DEFINE NODEGROUPMEMBER

Command	Description

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

DEFINE PATH (Define a path)

Use this command to define a path for a source to access a destination. Both the source and destination must be defined before you can define a path. For example, if a path is required between a server and a drive, you must first issue the DEFINE DRIVE command and then issue the DEFINE PATH command. A path must be defined after you issue the DEFINE DRIVE command in order to make the drive usable by the server.

Syntax and parameter descriptions are available for the following path types.

- DEFINE PATH (Define a path when the destination is a drive)
- DEFINE PATH (Define a path when the destination is a library)
- AIX Linux DEFINE PATH (Define a path when the destination is a ZOSMEDIA library)

For detailed and current device support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Related commands

Table 1. Commands related to DEFINE PATH

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE PATH	Deletes a path from a source to a destination.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DATAMOVER	Changes the definition for a data mover.
UPDATE PATH	Changes the attributes associated with a path.

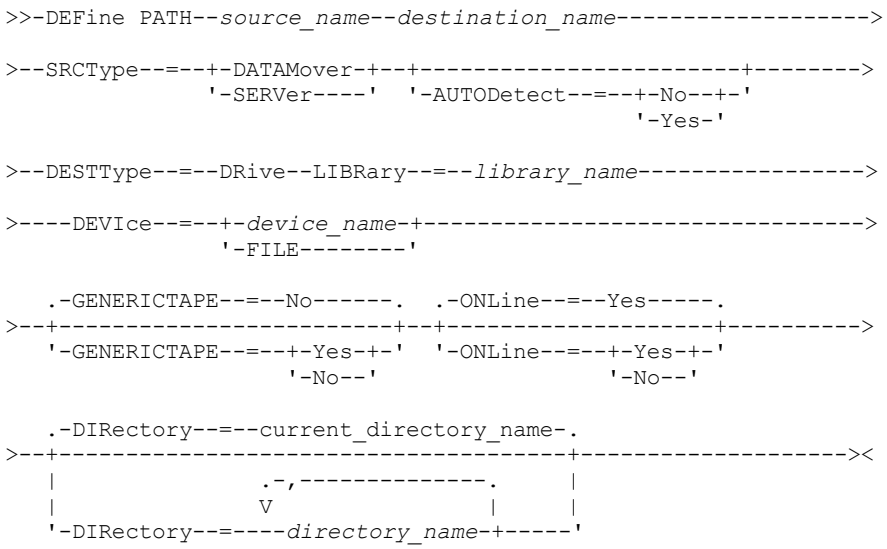
DEFINE PATH (Define a path when the destination is a drive)

Use this syntax when you define a path to a drive.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

source_name (Required)
: Specifies the name of source for the path. This parameter is required.

destination_name (Required)
: Specifies the name of the destination. This parameter is required.

SRCType (Required)
: Specifies the type of the source. This parameter is required. Possible values are:

  DATAMover
  : Specifies that a data mover is the source.

  SERVer
  : Specifies that a storage agent is the source.

AUTODetect
: Specifies whether the serial number for a drive is automatically updated in the database at the time that the path is defined. This parameter is optional. This parameter is only valid for paths that are defined from the local server to a drive. Possible values are:

  No
  : Specifies that the serial number is not automatically updated. The serial number is still compared with what is already in the database for the device. The server issues a message if there is a mismatch.

  Yes
  : Specifies that the serial number is not automatically updated to reflect the same serial number that the drive reports to the server.
  Important:

  1. If you did not set the serial number when you defined the drive, the server always tries to detect the serial number, and AUTODETECT defaults to YES. If you previously entered a serial number, then AUTODETECT defaults to NO.
  2. The use of AUTODETECT=YES in this command means that the serial number set in the drive definition is updated with the detected serial number.
  3. If you set DESTTYPE=DRIVE and AUTODETECT=YES, then the drive element number in the database is automatically changed to reflect the same element number that corresponds to the serial number of that drive. This is true for drives in a SCSI library. For more information about the element number, see DEFINE DRIVE.
  4. Depending on the capabilities of the device, the AUTODETECT parameter might not be supported.

DESTType=DRive (Required)
: Specifies that a drive is the destination. When the destination is a drive, you must specify a library name.

LIBRary
Specifies the name of the library to which the drive is assigned. The library and its drives must already be defined to the server. If the path is from a NAS data mover to a library, the library must have LIBTYPE of SCSI, 349X, or ACSLS.

DEVIce
Specifies the name of the device as known to the source, or FILE if the device is a logical drive in a FILE library.

AIX Windows The source uses the device name to access the drive. See Table 1 for examples.

Table 1. Examples of device names

Source to destination	Example

Server to a drive (not a FILE drive)	AIX
	`/dev/mt3`
	Windows
	`mt3`

Storage agent (on a Windows system) to a drive (not a FILE drive)	`mt3`
Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`
NAS data mover to a drive	NetApp NAS file server: `rst01` EMC Celerra NAS file server: `c436t011` IBM® System Storage® N Series: `rst01`

Linux The source uses the device name to access the drive. See Table 2 for examples.

Table 2. Examples of device names

Source to destination	Example
Server to a drive (not a FILE drive)	`/dev/tsmscsi/mt3`
Storage agent to a drive (not a FILE drive)	`/dev/tsmscsi/mt3`
Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`
NAS data mover to a drive	NetApp NAS file server: `rst01` EMC Celerra NAS file server: `c436t011` IBM System Storage N Series: `rst01`

Important:

- AIX Linux For 349X libraries, the alias name is a symbolic name that is specified in the /etc/ibmatl.conf file. Windows For 349X libraries, the alias name is a symbolic name that is specified in the c:\winnt\ibmatl.conf file. For more information, see *IBM Tape Device Drivers Installation and User's Guide*, which can be downloaded from the IBM Systems support site at http://www.ibm.com/support/docview.wss?uid=ssg1S7002972.
- For information about how to obtain names for devices that are connected to a NAS file server, consult the product information for the file server. For example, for a NetApp file server, connect to the file server using Telnet and issue the SYSCONFIG command. Use this command to determine device names for drives:

  ```
  sysconfig -t
  ```

Windows GENERICTAPE
Windows Specifies whether the tape drive to be used is a GENERICTAPE device class type. If the device is a tape drive and is not supported by IBM Spectrum Protect™ but is supported for the Windows operating system, you can use it with the generic tape format. To use the drive, specify GENERICTAPE=Yes when you define a path to the drive. The default is No. Possible values are:

Yes
Specifies that the tape drive to be used is a GENERICTAPE device class type.

No
Specifies that the tape drive to be used is not a GENERICTAPE device class type.

ONLine
Specifies whether the path is available for use. This parameter is optional. The default is YES. Possible values are:

Yes
Specifies that the path is available for use.

No
Specifies that the path is not available for use.

The source and the destination must both be available to use the path.

For example, if the path from a data mover to a drive is online, but either the data mover or the drive is offline, you cannot use the path.

DIRectory
Specifies the directory location or locations where the storage agent reads and writes the files that represent storage volumes for the FILE device class that is associated with the FILE library. The DIRECTORY parameter is also used for devices of type REMOVABLEFILE. For REMOVABLEFILE devices, the DIRECTORY parameter provides information for the server (not a storage agent) along with the DRIVE parameter to describe access to the device. This parameter is optional. For a path from a storage agent to a FILE device, this parameter is only valid when *all* of the following conditions are true:

- The source type is SERVER (meaning a storage agent that has been defined as a server to this server).
- The source name is the name of a storage agent, *not* the server.
- The destination is a logical drive that is part of a FILE library that is created when the device class was defined.

If you specified multiple directories for the device class associated with the FILE library, you must specify the same number of directories for each path to the FILE library. Do not change or move existing directories on the server that the storage agent is using so that the device class and the path remain synchronized. Adding directories is permitted. Specifying a mismatched number of directories can cause a runtime failure.

The default value for DIRECTORY is the directory of the server at the time the command is issued. The Windows registry is used to locate the default value.

Use a naming convention that you can use to associate the directory with a particular physical drive. This can help ensure that your configuration is valid for sharing the FILE library between the server and storage agent. If the storage agent is on a Windows system, use a universal naming convention (UNC) name. When the storage agent lacks permission to access remote storage, it experiences mount failures.

Windows The account that is associated with the storage agent service must either be an account within the local administrator's group or an account within the domain administrator's group. If the account is in the local administrator's group, the user ID and password must match that of an account with permissions to access storage as provided by the system that administers the remote share. For example, if a SAMBA server is providing access to remote storage, the user ID and password in the SAMBA configuration must match that of the local administrator user ID and password associated with the storage agent service.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path sta1 file1 srctype=server desttype=drive
library=file1 device=file
directory=\\192.168.1.10\filedir\dir1
```

In the previous example, the DEFINE DEVCLASS command establishes the shared file system in the directory that is accessed by the server as D:\FILEDIR\DIR1. The storage agent, however, is using UNC name \\192.168.1.10\FILEDIR\DIR1. This means that the system with TCP/IP address 192.168.1.10 is sharing the same directory using FILEDIR as the shared name. Also, the storage agent service has an account that can access this storage. It can access it either because it is associated with a local account with the same user ID and password as 192.168.1.10 or it is associated with a domain account that is available on both the storage agent and on 192.168.1.10. If appropriate to the installation, you can replace the 192.168.1.10 with a symbolic name such as:

```
example.yourcompany.com
```

Attention:

1. Storage agents access FILE volumes by replacing a directory name in a volume name with a directory name from a directory in the list provided with the DEFINE PATH command. Directories that are specified with this parameter are not validated on the server.
2. IBM Spectrum Protect does not create shares or permissions, or mount the target file system. You must complete these actions before you start the storage agent.

Example: Define a path from a server to a drive

Define a path from a server to a drive. In this case, the server name is *NET1*, the drive name is *TAPEDRV6*, the library is *NETLIB*, and the device name is *mt4*. Set AUTODETECT to NO.

```
define path net1 tapedrv6 srctype=server autodetect=no desttype=drive
    library=netlib device=mt4
```

Example: Define a path from a data mover server to a drive for backup and restore

Define a path from the data mover that is a NAS file server to the drive that the NAS file server will use for backup and restore operations. In this example, the NAS data mover is *NAS1*, the drive name is *TAPEDRV3*, the library is NASLIB, and the device name for the drive is *rst0l*.

```
define path nas1 tapedrv3 srctype=datamover desttype=drive library=naslib
    device=rst0l
```

Linux

Example: Define a path from a storage agent to a drive for backup and restore

Define a path from storage agent *SA1* to the drive that the storage agent uses for backup and restore operations. In this example, the library is *TSMLIB*, the drive is *TAPEDRV4*, and the device name for the drive is /dev/tsmscsi/mt3.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
    device=/dev/tsmscsi/mt3
```

AIX Windows

Example: Define a path from a storage agent to a drive for backup and restore

Define a path from storage agent *SA1* to the drive that the storage agent uses for backup and restore operations. In this example, the library is *TSMLIB*, the drive is *TAPEDRV4*, and the device name for the drive is /dev/mt3.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
    device=/dev/mt3
```

AIX Windows

Example: Define a path to give a storage agent access to shared disk storage

Define a path that gives the storage agent access to files on disk storage that is shared with the server. Drive *FILE9* is defined to library *FILE1* on the server. The storage agent *SA1* accesses *FILE9*. On the storage agent, this data is on directory \\192.168.1.10\filedata.

AIX The data for *FILE9* resides on the server at /tsmdata/filedata.

Windows The data for *FILE9* resides on the server at d:\tsmdata\filedata.

```
define path sa1 file9 srctype=server desttype=drive library=file1 device=file
    directory="\\192.168.1.10\filedata"
```

Example: Configure a storage agent to use a FILE library

The following example illustrates the importance of matching device classes and paths to ensure that storage agents can access newly created FILE volumes.

Suppose you want to use these three directories for a FILE library: Windows

- c:\server
- d:\server
- e:\server

AIX Linux

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Use the following command to set up a FILE library named CLASSA with one drive named CLASSA1 on SERVER1: Windows

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

AIX Linux

```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```

2. You want the storage agent STA1 to be able to use the FILE library, so you define the following path for storage agent STA1:

Windows

```
define path sta1 classa1 srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

AIX Linux

```
define path sta1 classa1 srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

Windows In this scenario, the storage agent, STA1, replaces the directory name c:\server with the directory name \\192.168.1.10\c\server to access FILE volumes that are in the c:\server directory on the server.

AIX Linux In this scenario, the storage agent, STA1, replaces the directory name /opt/tivoli1 with the directory name /opt/ibm1/ to access FILE volumes that are in the /opt/tivoli1 directory on the server.

3. Windows File volume c:\server\file1.dsm is created by SERVER1. If you later change the first directory for the device class with the following command:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

SERVER1 is still able to access file volume c:\server\file1.dsm, but the storage agent STA1 is not able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list that is associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume is still accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.

4. If file volume /opt/tivoli1/file1.dsm is created on SERVER1, and if the following command is issued,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

SERVER1 is still able to access file volume /opt/tivoli1/file1.dsm, but the storage agent STA1 is not able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list that is associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume is still accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.

DEFINE PATH (Define a path when the destination is a library)

Use this syntax when defining a path to a library.

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine PATH--source_name--destination_name------------------->

                          (1)
>--SRCType--=--+-DATAMover-----+--+-----------------------+---->
               '-SERVer--------'  '-AUTODetect--=--+-No--+-'
                                                  '-Yes-'

>--DESTType--=--LIBRary--+-DEVIce--=--device_name--------+------>
                         '-EXTERNALManager--=--path_name-'
```

```
   .-ONLine--=--Yes-----.
>--+--------------------+-------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Notes:

1. DATAMOVER only applies to NAS devices.

Parameters

source_name (Required)
: Specifies the name of source for the path. This parameter is required.

destination_name (Required)
: Specifies the name of the destination. This parameter is required.
: Attention: To define a path from a NAS data mover to a library, the library must have LIBTYPE of SCSI, 349x, or ACSLS.

SRCType (Required)
: Specifies the type of the source. This parameter is required. Possible values are:

: DATAMover
: : Specifies that a data mover is the source.
: SERVer
: : Specifies that a storage agent is the source.

AUTODetect
: Specifies whether the serial number for a drive or library will be automatically updated in the database at the time that the path is defined. This parameter is optional. This parameter is only valid for paths defined from the local server to a drive or a library. Possible values are:

: No
: : Specifies that the serial number will not be automatically updated. The serial number is still compared with what is already in the database for the device. The server issues a message if there is a mismatch.
: Yes
: : Specifies that the serial number will be automatically updated to reflect the same serial number that the drive reports to IBM Spectrum Protect™.
: : Important:

: : 1. If you did not set the serial number when you defined the drive or the library, the server always tries to detect the serial number, and AUTODETECT defaults to YES. If you have previously entered a serial number, then AUTODETECT defaults to NO.
: : 2. The use of AUTODETECT=YES in this command means that the serial number set in the drive or library definition is updated with the detected serial number.
: : 3. Depending on the capabilities of the device, the AUTODETECT parameter may not be supported.

DESTType=LIBRary (Required)
: Specifies that a library is the destination. This parameter is required.

DEVIce
: Specifies the name of the device as known to the source, or FILE if the device is a logical drive in a FILE library.
: AIX Windows The source uses the device name to access the library. See Table 1 for examples.

Table 1. Examples of device names

Source to destination	Example

Server to a library	AIX
	`/dev/lb4`
	Linux
	`/dev/tsmscsi/lb4`
	Windows
	`lb4.1`

Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`

Source to destination	Example
NAS data mover to a library	`mc0`

Linux The source uses the device name to access the library. See Table 2 for examples.

Table 2. Examples of device names

Source to destination	Example
Server to a library	`/dev/tsmscsi/lb4`
NAS data mover to a library	`mc0`

Important:

- AIX Linux For 349X libraries, the alias name is a symbolic name that is specified in the /etc/ibmatl.conf file. Windows For 349X libraries, the alias name is a symbolic name that is specified in the c:\winnt\ibmatl.conf file. For more information, see *IBM Tape Device Drivers Installation and User's Guide*, which can be downloaded from the IBM® Systems support site at http://www.ibm.com/support/docview.wss?uid=ssg1S7002972.
- For information about how to obtain names for devices that are connected to a NAS file server, consult the product information for the file server. For example, for a NetApp file server, connect to the file server using Telnet and issue the SYSCONFIG command. Use this command to determine device names for drives:

  ```
  sysconfig -t
  ```

  Use this command to determine the device name for a library:

  ```
  sysconfig -m
  ```

EXTERNALManager

Specifies the location of the external library manager where IBM Spectrum Protect can send media access requests. Use single quotation marks around the value of this parameter. For example, enter: AIX

```
/usr/lpp/GESedt-acsls/bin/elmdt
```

Linux

```
/opt/GESedt-acsls/bin/elmdt
```

Windows

```
C:\Program Files\GES\EDT-ACSLS\bin\elmdt.exe
```

This parameter is required when the library name is an external library.

ONLine

Specifies whether the path is available for use. This parameter is optional. The default is YES. Possible values are:

Yes
: Specifies that the path is available for use.

No
: Specifies that the path is not available for use.

The source and the destination must both be available to use the path.

Attention: If the path to a library is offline, the server will not be able to access the library. If the server is halted and restarted while the path to the library is offline, the library will not be initialized.

Example: Define a path from a server to a library

Define a path from the server SATURN to the SCSI type library SCSILIB: AIX

```
define path saturn scsilib srctype=server
desttype=library device=/dev/lb3
```

Linux

```
define path saturn scsilib srctype=server
desttype=library device=/dev/tsmscsi/lb3
```

Windows

```
define path saturn scsilib srctype=server
desttype=library device=lb3.0.0.0
```

AIX | Linux

DEFINE PATH (Define a path when the destination is a ZOSMEDIA library)

Use this syntax when defining a path to a ZOSMEDIA library. You must first define the z/OS® media server in your configuration with the DEFINE SERVER command.

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DEFine PATH--source_name--destination_name------------------->

>--SRCType--=--SERVer--DESTType--=--LIBRary--------------------->

                                  .-ONLine--=--Yes-----.
>--ZOSMEDIASERVER--=--server_name--+--------------------+------><
                                  '-ONLine--=--+-Yes-+-'
                                               '-No--'
```

Parameters

source_name (Required)
: Specifies the name of source for the path.

destination_name (Required)
: Specifies the name of the ZOSMEDIA library.

SRCType=SERVer (Required)
: Specifies that a storage agent or server is the source.

DESTType=LIBRary (Required)
: Specifies that a library is the destination.

ZOSMEDIAServer (Required)
: Specifies the name of the server that represents a Tivoli® Storage Manager for z/OS Media server.

ONLine
: Specifies whether the path is available for use. This parameter is optional. The default is YES. Possible values are:

  Yes
  : Specifies that the path is available for use.

  No
  : Specifies that the path is not available for use.

  The source and the destination must both be available to use the path.

  Attention: If the path to a library is offline, the server will not be able to access the library. If the server is halted and restarted while the path to the library is offline, the library will not be initialized.

  If the z/OS media server cannot be accessed during initialization of the IBM Spectrum Protect™ server, the library path will be set offline. Use the UPDATE PATH command and specify ONLINE=YES to vary the ZOSMEDIA library back online.

DEFINE POLICYSET (Define a policy set)

Use this command to define a policy set in a policy domain. A policy set contains management classes, which contain copy groups. You can define one or more policy sets for each policy domain.

To put a policy set into effect, you must activate the policy set by using the ACTIVATE POLICYSET command. Only one policy set can be active in a policy domain. The copy groups and management classes within the active policy set determine the rules by which client nodes perform backup, archive, and space management operations, and how the client files stored are managed.

Use the VALIDATE POLICYSET command to verify that a policy set is complete and valid before activating it with the ACTIVATE POLICYSET command.

Privilege class

To issue this command you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-DEFine POlicyset--domain_name--policy_set_name--------------->

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the policy set belongs.

policy_set_name (Required)
: Specifies the name of the policy set. The maximum length of this name is 30 characters. You cannot define a policy set named ACTIVE.

DESCription
: Specifies a description for the new policy set. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Example: Define a policy set

Define a policy set called `SUMMER` for the `PROG1` policy domain and include the description, "Programming Group Policies."

```
define policyset prog1 summer
description="Programming Group Policies"
```

Related commands

Table 1. Commands related to DEFINE POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY MGMTCLASS	Creates a copy of a management class.
COPY POLICYSET	Creates a copy of a policy set.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DEFINE MGMTCLASS	Defines a management class.
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY POLICYSET	Displays information about policy sets.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

DEFINE PROFASSOCIATION (Define a profile association)

Use this command on a configuration manager to associate one or more objects with a configuration profile for distribution to subscribing managed servers. After a managed server subscribes to a profile, the configuration manager sends object definitions associated with the profile to the managed server where they are stored in the database. Objects created this way in the database of a managed server become managed objects. An object can be associated with more than one profile.

You can use this command to define an initial set of profile associations and to add to existing associations.

You can associate the following types of objects with a profile:

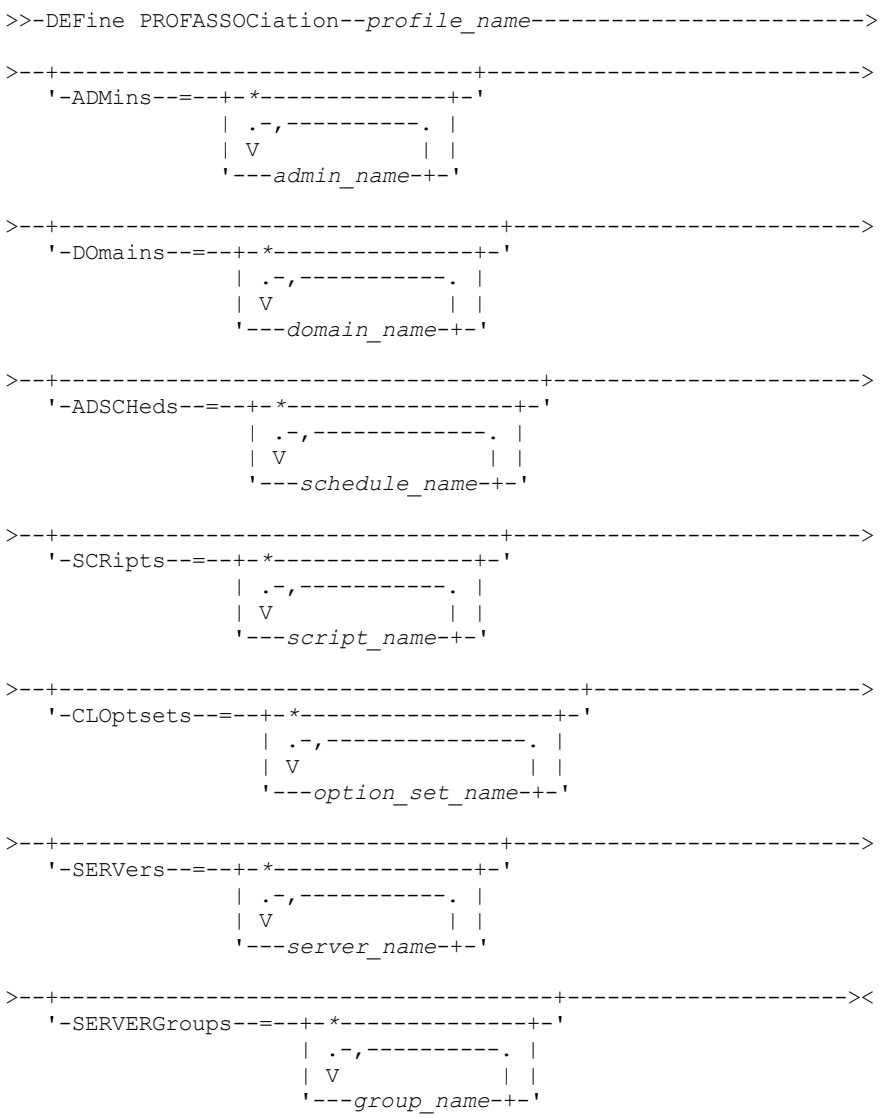
- Administrator registrations and authorities
- Policy domains, which include the domains' policy sets, management classes, copy groups, and client schedules
- Administrative schedules
- Server command scripts
- Client option sets
- Server definitions
- Server group definitions

Tip: The configuration manager does not distribute status information for an object to managed servers. For example, information such as the number of days since an administrator last accessed the server is not distributed to managed servers. This type of information is maintained in the databases of the individual managed servers.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

profile_name (Required)
Specifies the name of the configuration profile.

ADMins
Specifies administrators to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all administrators that are registered with the configuration manager. If you specify the match-all definition and later add more administrators, they are automatically distributed through the profile.
The configuration manager distributes the administrator name, password, contact information, and authorities of administrators associated with the profile. The configuration manager does not distribute the following:

- The administrator named SERVER_CONSOLE, even if you use a match-all definition
- The locked or unlocked status of an administrator

When the profile already has administrators associated with it, the following apply:

- If you specify a list of administrators and a list already exists, IBM Spectrum Protect™ combines the new list with the existing list.
- If you specify a match-all definition and a list of administrators already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of administrators, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the ADMINS=* parameter.

DOmains
Specifies policy domains to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all domains that are defined on the configuration manager. If you specify the match-all definition and later add more domains, they are automatically distributed through the profile.

The configuration manager distributes domain information that includes definitions of policy domains, policy sets, management classes, copy groups, and client schedules. The configuration manager does not distribute the ACTIVE policy set. Administrators on a managed server can activate any policy set within a managed domain on a managed server.

When the profile already has domains associated with it, the following apply:

- If you specify a list of domains and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of domains already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of domains, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the DOMAINS=* parameter.

Important: Client operations such as backup and archive fail if destination pools do not exist. Therefore, managed servers that subscribe to this profile must have definitions for any storage pools specified as destinations in the associated domains. Use the RENAME STGPOOL command to rename existing storage pools to match the destination names distributed.

ADSCHeds
Specifies administrative schedules to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all administrative schedules that are defined on the configuration manager. If you specify the match-all definition and later add more administrative schedules, they are automatically distributed through the profile.
Tip: Administrative schedules are not active when they are distributed by a configuration manager. An administrator on a managed server must activate any schedule to have it run on that server.
When the profile already has administrative schedules associated with it, the following apply:

- If you specify a list of administrative schedules and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of administrative schedules already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of administrative schedules, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the ADSCHEDS=* parameter.

SCRipts
Specifies server command scripts to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all scripts that are defined on the configuration manager. If you specify the match-all definition and later add more scripts, they are automatically distributed through the profile.
When the profile already has scripts associated with it, the following apply:

- If you specify a list of scripts and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of scripts already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of scripts, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the SCRIPTS=* parameter.

CLOptsets
Specifies client option sets to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all client option sets that are defined on the configuration manager. If you specify the match-all definition and later add more client option sets, they are automatically distributed through the profile.
When the profile already has client option sets associated with it, the following apply:

- If you specify a list of client option sets and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of client option sets already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of client option sets, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the CLOPSETS=* parameter.

SERVers
Specifies server definitions to associate with the profile. The definitions are distributed to managed servers that subscribe to this profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk (*) by itself, to specify all servers that are defined on the configuration manager. If you specify the match-all definition and later add more servers, they are automatically distributed through the profile.

The configuration manager distributes the following server attributes: communication method, IP address, port address, server password, URL, and the description. Distributed server definitions always have the ALLOWREPLACE attribute set to YES on the managed server, regardless of this parameter's value on the configuration manager. On the managed server, you can use the UPDATE SERVER command to set all other attributes.

When the profile already has servers associated with it, the following apply:

- If you specify a list of servers and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of servers already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of servers, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the SERVERS=* parameter.

Important:

1. A server definition on a managed server is not replaced by a definition from the configuration manager unless you have allowed replacement of the definition on the managed server. To allow replacement, on the managed server update the server definition by using the UPDATE SERVER command with ALLOWREPLACE=YES.
2. If a configuration manager distributes a server definition to a managed server, and a server group of the same name exists on the managed server, the distributed server definition replaces the server group definition.

SERVERGroups
Specifies server groups to associate with the profile. You can use wildcard characters in the names. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all definition, an asterisk

(*) by itself, to specify all server groups that are defined on the configuration manager. If you specify the match-all definition and later add more server groups, they are automatically distributed through the profile.
Tip: A configuration manager does not distribute a server group definition to a managed server if the managed server has a server defined with the same name as that of the server group.
When the profile already has server groups associated with it, the following apply:

- If you specify a list of server groups and a list already exists, IBM Spectrum Protect combines the new list with the existing list.
- If you use a match-all definition and a list of server groups already exists, IBM Spectrum Protect replaces the list with the match-all definition.
- If you specify a list of server groups, and a match-all definition had previously been specified, IBM Spectrum Protect ignores the list. To remove the match-all definition, issue the DELETE PROFASSOCIATION command with the SERVERGROUPS=* parameter.

Example: Associate a specific domain with a specific profile

Associate a domain named MARKETING with a profile named DELTA.

```
define profassociation delta domains=marketing
```

Example: Associate all domains with a specific profile

You have already associated a list of domains with a profile named GAMMA. Now associate all domains defined on the configuration manager with the profile.

```
define profassociation gamma domains=*
```

Related commands

Table 1. Commands related to DEFINE PROFASSOCIATION

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

DEFINE PROFILE (Define a profile)

Use this command on a configuration manager to define a profile (a set of configuration information) that can be distributed to managed servers.

After defining a profile, you can use the DEFINE PROFASSOCIATION command to specify objects to be distributed to managed servers subscribing to the profile.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine PROFIle--profile_name--------------------------------->

>--+----------------------------+---------------------------><
   '-DESCription--=--description-'
```

Parameters

profile_name (Required)
: Specifies the name of the profile. The maximum length of the name is 30 characters.

DESCription
: Specifies a description of the profile. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. This parameter is optional.

Example: Define a new profile

Define a profile named ALPHA with a description of "Programming Center."

```
define profile alpha
description="Programming Center"
```

Related commands

Table 1. Commands related to DEFINE PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

DEFINE RECMEDMACHASSOCIATION (Associate recovery media with a machine)

Use this command to associate recovery media with one or more machines. A machine is associated with recovery media so that the location of the boot media and its list of volume names are available to recover the machine. To retrieve the information, issue the QUERY MACHINE command. This information will be included in the plan file to help you recover the client machines.

To associate a machine with recovery media, both the machine and media must be defined to IBM Spectrum Protect™. A machine remains associated with the media until the association, the media, or the machine is deleted.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                    .-,------------.
                    V              |
```

```
>>-DEFine RECMEDMACHAssociation--media_name----machine_name-+-->
```

Parameters

media_name (Required)
: Specifies the name of the recovery media with which one or more machines will be associated.

machine_name (Required)
: Specifies the name of the machines to be associated with the recovery media. A machine can be associated with multiple recovery media. To specify a list of machines, separate the names with commas and no intervening spaces. You can use wildcard characters to specify a name.

Example: Associate machines to recovery media

Associate machines DISTRICT1 and DISTRICT5 to the DIST5RM recovery media.

```
define recmedmachassociation dist5rm
district1,district5
```

Related commands

Table 1. Commands related to DEFINE RECMEDMACHASSOCIATION

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
DEFINE RECOVERYMEDIA	Defines the media required to recover a machine.
DELETE MACHINE	Deletes a machine.
DELETE RECMEDMACHASSOCIATION	Deletes association between recovery media and a machine.
DELETE RECOVERYMEDIA	Deletes recovery media.
QUERY MACHINE	Displays information about machines.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.

DEFINE RECOVERYMEDIA (Define recovery media)

Use this command to define the media needed to recover a machine. The same media can be associated with multiple machines. To display the information, use the QUERY MACHINE command. This information will be included in the plan file to help you to recover the client machines.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine RECOVERYMedia--media_name----------------------------->

>--+---------------------------------+-------------------------->
   |                 .-,-----------. |
   |                 V             | |
   '-VOLumenames--=----volume_name-+-'

>--+-----------------------------+--+-----------------------+--->
   '-DESCription--=--description-'  '-LOcation--=--location-'

   .-Type--=--OTher-----.
>--+--------------------+--+-------------------------+--------->
   '-Type--=--+-OTher-+-'  '-PROduct--=--product_name-'
              '-BOot--'

>--+-------------------------------------+--------------------><
```

```
'-PRODUCTInfo--=--product_information-'
```

Parameters

media_name (Required)
: Specifies the name of the recovery media to be defined. The name can be up to 30 characters.

VOLumenames
: Specifies the names of volumes that contain the recoverable data (for example, operating system image copies). This parameter is required if you specify a media type of BOOT. Specify boot media volume names in the order in which they are to be inserted into the machine at recovery time. The maximum length of the volume names list is 255 characters. Enclose the list in quotation marks if it contains any blank characters.

DESCription
: Specifies the description of the recovery media. This parameter is optional. The maximum length is 255 characters. Enclose the text in quotation marks if it contains any blank characters.

LOcation
: Specifies the location of the recovery media. This parameter is optional. The maximum length is 255 characters. Enclose the text in quotation marks if it contains any blank characters.

Type
: Specifies the type of recovery media. This parameter is optional. The default is OTHER.

  BOot
  : Specifies that this is boot media. You must specify volume names if the type is BOOT.

  OTher
  : Specifies that this is not boot media. For example, a CD that contains operating system manuals.

PROduct
: Specifies the name of the product that wrote to this media. This parameter is optional. The maximum length is 16 characters. Enclose the text in quotation marks if it contains any blank characters.

PRODUCTInfo
: Specifies information about the product that wrote to the media. This would be information that you may need to restore the machine. This parameter is optional. The maximum length is 255 characters. Enclose the text in quotation marks if it contains any blank characters.

Example: Define the media needed to recover a machine

Define the recovery media named DIST5RM. Include a description and the location.

```
define recoverymedia dist5rm
description="district 5 base system image"
location="district 1 vault"
```

Related commands

Table 1. Commands related to DEFINE RECOVERYMEDIA

Command	Description
DEFINE RECMEDMACHASSOCIATION	Associates recovery media with a machine.
DELETE RECOVERYMEDIA	Deletes recovery media.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.
UPDATE RECOVERYMEDIA	Changes the attributes of recovery media.

DEFINE SCHEDULE (Define a client or an administrative command schedule)

Use this command to create a client or administrative command schedule.

The DEFINE SCHEDULE command takes two forms: one if the schedule applies to client operations, one if the schedule applies to administrative commands. Within these two forms, you can select either classic or enhanced style schedules. The syntax and

parameters for each form are defined separately.

For each schedule, a startup window is specified. The startup window is the time period during which the schedule must be initiated. The schedule will not necessarily complete processing within this window. If the server is not running when this window starts, but is started before the end of the defined window is reached, the schedule will run when the server is restarted. Options associated with each schedule style (classic and enhanced) determine when the startup windows should begin.

Table 1. Commands related to DEFINE SCHEDULE

Command	Description
COPY SCHEDULE	Creates a copy of a schedule.
DEFINE ASSOCIATION	Associates clients with a schedule.
DELETE SCHEDULE	Deletes a schedule from the database.
QUERY EVENT	Displays information about scheduled and completed events for selected clients.
QUERY SCHEDULE	Displays information about schedules.
SET MAXCMDRETRIES	Specifies the maximum number of retries after a failed attempt to execute a scheduled command.
SET MAXSCHEDSESSIONS	Specifies the maximum number of client/server sessions available for processing scheduled work.
SET RETRYPERIOD	Specifies the time between retry attempts by the client scheduler.
UPDATE SCHEDULE	Changes the attributes of a schedule.

- DEFINE SCHEDULE (Define a client schedule)
  Use the DEFINE SCHEDULE command to define a client schedule. IBM Spectrum Protect uses this schedule to automatically perform a variety of client operations for your client workstation at specified intervals or days. After you define a schedule, use the DEFINE ASSOCIATION command to associate the client with the schedule.
- DEFINE SCHEDULE (Define a schedule for an administrative command)
  Use the DEFINE SCHEDULE command to create a new schedule for processing an administrative command.

DEFINE SCHEDULE (Define a client schedule)

Use the DEFINE SCHEDULE command to define a client schedule. IBM Spectrum Protect™ uses this schedule to automatically perform a variety of client operations for your client workstation at specified intervals or days. After you define a schedule, use the DEFINE ASSOCIATION command to associate the client with the schedule.

You must start the client scheduler on the client workstation for IBM Spectrum Protect to process the schedule.

Not all clients can run all scheduled operations, even though you can define the schedule on the server and associate it with the client. For example, a Macintosh client cannot run a schedule when the action is to restore or retrieve files, or run an executable script. An executable script is also known as a command file, a batch file, or a script on different client operating systems.

IBM Spectrum Protect cannot run multiple schedules concurrently for the same client node.

Privilege class

To define a client schedule, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the schedule belongs.

Syntax

Classic client schedule

```
>>-DEFine SCHedule--domain_name--schedule_name------------------>

>--+-----------------+--+-----------------------------+--------->
   '-Type--=--Client-'  '-DESCription--=--description-'
```


.-ACTion--=--Incremental----------.
'-ACTion--=--+-Incremental-+-'
+-Selective-+
+-Archive--+-+
+-Backup--+-+
'-REStore-+
'-RETrieve-+
'-IMAGEBACkup-+
'-IMAGEREStore-+
'-Command-+
'-Macro-+
'-Deploy-'
SUBACTion--=--
FASTBack-'
FASTBack----+
SYSTEMSTate-+
VApp--------+
'-VM----------'
>--+-------------------------+-->
'-OPTions--=--option_string-'
.-PRIority--=--5------.
>--+-------------------+--+---------------------+--->
| (1) | '-PRIority--=--number-'
'-OBJects------=--object_string-'
.-STARTDate--=--current_date-.
>--+-----------------------------+-->
'-STARTDate--=--date---------'
.-STARTTime--=--current_time-. .-DURation--=--1------.
>--+---------------------------+--+---------------------+------>
'-STARTTime--=--time---------' '-DURation--=--number-'
.-DURUnits--=--Hours----------. .-MAXRUNtime--=--0------.
>--+-----------------------------+--+-----------------------+--->
'-DURUnits--=--+-Minutes----+-' '-MAXRUNtime--=--number-'
+-Hours------+
+-Days-------+
'-INDefinite-'
.-SCHEDStyle--=--Classic-. .-PERiod--=--1------.
>--+-----------------------+--+-------------------+------------>
'-SCHEDStyle--=--Classic ' '-PERiod--=--number-'
.-PERUnits--=--Days--------.
>--+-------------------------+-------------------------------->
'-PERUnits--=--+-Hours---+-'
+-Days----+
+-Weeks---+
+-Months--+
+-Years---+
'-Onetime-'
.-DAYofweek--=--ANY-----------.
>--+-----------------------------+------------------------------>
'-DAYofweek--=--+-ANY-------+-'
+-WEEKDay---+
+-WEEKEnd---+
+-SUnday----+
+-Monday----+
+-TUesday---+
+-Wednesday-+
+-THursday--+
+-Friday----+
'-SAturday--'
.-EXPiration--=--Never-----.

```
>--+-------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-date--'
```

Notes:

1. The OBJECTS parameter is optional when `ACTION=INCREMENTAL`, but is required for other actions.

Syntax

```
Enhanced client schedule

>>-DEFine SCHedule--domain_name--schedule_name----------------->

>--+-----------------+--+----------------------------+--------->
   '-Type--=--Client-'  '-DESCription--=--description-'

   .-ACTion--=--Incremental---------------------------------.
>--+-----------------------------------------------------------+-->
   '-ACTion--=--+-Incremental-------------------------------+-'
                +-Selective-----------------------------------+
                +-Archive--+-------------------------+-------+
                |          '-SUBACTion--=--FASTBack-'       |
                +-Backup--+-------------------------------+-+
                |         |               .-""----------. | |
                |         '-SUBACTion--=--+-------------+-' |
                |                         +-FASTBack----+   |
                |                         +-SYSTEMSTate-+   |
                |                         +-VApp--------+   |
                |                         '-VM----------'   |
                +-REStore-------------------------------------+
                +-RETrieve------------------------------------+
                +-IMAGEBACkup---------------------------------+
                +-IMAGEREStore--------------------------------+
                +-Command-------------------------------------+
                '-Macro-----------------------------------------'

>--+-------------------------+-------------------------------->
   '-OPTions--=--option_string-'

                                    .-PRIority--=--5------.
>--+-------------------------------+--+--------------------+--->
   |         (1)                   |  '-PRIority--=--number-'
   '-OBJects------=--object_string-'

   .-STARTDate--=--current_date-.
>--+---------------------------+------------------------------->
   '-STARTDate--=--date---------'

   .-STARTTime--=--current_time-.  .-DURation--=--1------.
>--+---------------------------+--+--------------------+------>
   '-STARTTime--=--time---------'  '-DURation--=--number-'

   .-DURUnits--=--Hours-------.  .-MAXRUNtime--=--0------.
>--+-------------------------+--+-----------------------+------>
   '-DURUnits--=--+-Minutes-+-'  '-MAXRUNtime--=--number-'
                  +-Hours---+
                  '-Days----'

                            .-MONth--=--ANY-----------.
>--SCHEDStyle--=--Enhanced--+-------------------------+--------->
                            '-MONth--=--+-ANY-------+-'
                                        +-JAnuary---+
                                        +-February--+
                                        +-MARch-----+
                                        +-APril-----+
                                        +-May-------+
                                        +-JUNe------+
                                        +-JULy------+
                                        +-AUgust----+
                                        +-September-+
```

```
                                        +-October---+
                                        +-November--+
                                        '-December--'

   .-DAYOFMonth--=--ANY-----.  .-WEEKofmonth--=--ANY--------.
>--+-----------------------+--+---------------------------+--->
   '-DAYOFMonth--=--+-ANY-+-'  '-WEEKofmonth--=--+-ANY----+-'
                    '-Day-'                      +-FIrst--+
                                                 +-Second-+
                                                 +-Third--+
                                                 +-FOurth-+
                                                 '-Last---'

   .-DAYofweek--=--ANY-----------.
>--+---------------------------+-----------------------------><
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

   .-EXPiration--=--Never-----.
>--+-------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-date--'
```

Notes:

1. The OBJECTS parameter is optional when `ACTION=INCREMENTAL`, but is required for other actions.

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which this schedule belongs.

schedule_name (Required)
: Specifies the name of the schedule to be defined. You can specify up to 30 characters for the name.

Type=Client
: Specifies that a schedule for a client is defined. This parameter is optional.

DESCription
: Specifies a description of the schedule. This parameter is optional. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains any blank characters.

ACTion
: Specifies the action that occurs when this schedule is processed. Possible values are:

  Incremental
  : Specifies that the schedule backs up all files that are new or that have changed since the last incremental backup. Incremental also backs up any file for which all existing backups might have expired.

  Selective
  : Specifies that the schedule backs up only files that are specified with the OBJECTS parameter.

  Archive
  : Specifies that the schedule archives files that are specified with the OBJECTS parameter.

  Backup
  : Specifies that the schedule backs up files that are specified with the OBJECTS parameter.

  REStore
  : Specifies that the schedule restores files that are specified with the OBJECTS parameter.

    When you specify ACTION=RESTORE for a scheduled operation, and the REPLACE option is set to PROMPT, no prompting occurs. If you set the option to PROMPT, the files are skipped.

    If you specify a second file specification, this second file specification acts as the restore destination. If you need to restore multiple groups of files, schedule one for each file specification that you need to restore.

RETrieve
: Indicates that the schedule retrieves files that are specified with the OBJECTS parameter.
Remember: A second file that is specified acts as the retrieve destination. If you need to retrieve multiple groups of files, create a separate schedule for each group of files.

IMAGEBACkup
: Specifies that the schedule backs up logical volumes that are specified with the OBJECTS parameter.

IMAGEREStore
: Specifies that the schedule restores logical volumes that are specified with the OBJECTS parameter.

Command
: Specifies that the schedule processes a client operating system command or script that is specified with the OBJECTS parameter.

Macro
: Specifies that a client processes a macro whose file name is specified with the OBJECTS parameter.

SUBACTion
: You can specify one of the following values:

  ""
  : When a null string (two double quotes) is specified with ACTION=BACKUP the backup is an incremental.

  FASTBAck
  : Specifies that a FastBack client operation that is identified by the ACTION parameter is to be scheduled for processing. The ACTION parameter must be either ARCHIVE or BACKUP.

  SYSTEMSTate
  : Specifies that a client Systemstate backup is scheduled.

  VApp
  : Specifies that a client vApp backup is scheduled. A vApp is a collection of pre-deployed virtual machines.

  VM
  : Specifies that a client VMware backup operation is scheduled.

Deploy
: Specifies whether to update client workstations with deployment packages that are specified with the OBJECTS parameter. The OBJECTS parameter must contain two specifications, the package files to retrieve and the location from which to retrieve them. Ensure that the objects are in the order *`files location`*. For example:

  ```
  define schedule standard deploy_1 action=DEPLOY objects=
  "\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\*
  ..\IBM_ANR_WIN\"
  ```

  Values for the following options are restricted when you specify ACTION=DEPLOY:

  PERUNITS
  : Specify `PERUNITS=ONETIME`. If you specify `PERUNITS=PERIOD`, the parameter is ignored.

  DURUNITS
  : Specify `MINUTES`, `HOURS`, or `DAYS` for the DURUNITS parameter. Do not specify INDEFINITE.

  SCHEDSTYLE
  : Specify the default style, CLASSIC.

  The SCHEDULE command fails if the parameters do not conform to the required parameter values, such as the V.R.M.F.

OPTions
: Specifies the client options that you specify to the scheduled command at the time the schedule is processed. This parameter is optional.
Only those options that are valid on the scheduled command can be specified for this parameter. Refer to the appropriate client manual for information about options that are valid from the command line. All options described there as valid only on the initial command line result in an error or are ignored when running the schedule from the server. For example, do not include the following options because they have no effect when the client processes the scheduled command:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME

- TCPCLIENTADDRESS
- TCPCLIENTPORT

Windows When you define a scheduler service by using the DSMCUTIL command or the backup-archive client GUI wizard, you specify an options file. You cannot override the options in that options file by issuing the scheduled command. You must modify the options in your scheduler service.

If the option string contains multiple options or options with embedded spaces, surround the entire option string with one pair of apostrophes. Enclose individual options that contain spaces in quotation marks. A leading minus sign is required in front of the option. Errors can occur if the option string contains spaces that are not quoted correctly.

The following examples show how to specify some client options:

- To specify `subdir=yes` and `domain all-local -systemobject`, enter:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- To specify `domain all-local -c: -d:`, enter:
  - `options='-domain="all-local -c: -d:"'`

Windows Tip:

For Windows clients running in batch mode, if the use of quotation marks is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

- Processing a series of commands from the administrative client
- Processing individual commands from the administrative client

OBJects

Specifies the objects for which the specified action is performed. Use a single space between each object. This parameter is required except when ACTION=INCREMENTAL. If the action is a backup, archive, retrieve, or restore operation, the objects are file spaces, directories, or logical volumes. If the action is to run a command or macro, the object is the name of the command or macro to run.

When you specify ACTION=INCREMENTAL without specifying a value for this parameter, the scheduled command is invoked without specified objects and attempts to process the objects as defined in the client option file. To select all file spaces or directories for an action, explicitly list them in the object string. Entering only an asterisk in the object string causes the backup to occur only for the directory where the scheduler was started.

Important:

- If you specify a second file specification, and it is not a valid destination, you receive this error:

  ```
  ANS1082E Invalid destination file specification <filespec> entered.
  ```

- If you specify more than two file specifications, you receive this error:

  ```
  ANS1102E Excessive number of command line arguments passed to the
  program!
  ```

When you specify ACTION=ARCHIVE, INCREMENTAL, or SELECTIVE for this parameter, you can list a maximum of twenty (20) file specifications.

Enclose the object string in double quotes if it contains blank characters (spaces), and then surround the double quotes with single quotes. If the object string contains multiple file names, enclose each file name with its own pair of double quotes, then surround the entire string with one pair of single quotes. Errors can occur if file names contain a space that is not quoted correctly.

Windows If you are using characters that have a special meaning for Windows users, such as commas, surround the entire argument in two pairs of double quotes, then surround the entire string with single quotes. The following examples show you how to specify some file names:

- To specify C:\FILE 2, D:\GIF FILES, and E:\MY TEST FILE, enter:
  - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
- To specify D:\TEST FILE, enter:
  - `OBJECTS='"D:\TEST FILE"'`
- To specify D:TEST,FILE:
  - `OBJECTS='""D:\TEST,FILE""'`

AIX Linux The following examples show how to specify some file names:

- To specify /home/file 2, /home/gif files, and /home/my test file, enter:
  - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
- To specify /home/test file, enter:
  - `OBJECTS='"/home/test file"'`

Windows Tip:

For Windows clients running in batch mode, if the use of double quotes is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

- Processing a series of commands from the administrative client
- Processing individual commands from the administrative client

PRIority

Specifies the priority value for a schedule. This parameter is optional. You can specify an integer from 1 to 10, with 1 being the highest priority and 10 being the lowest. The default is 5.

If two or more schedules have the same window start time, the value you specify determines when IBM Spectrum Protect processes the schedule. The schedule with the highest priority starts first. For example, a schedule with PRIORITY=3 starts before a schedule with PRIORITY=5.

STARTDate

Specifies the date for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current date. Use this parameter with the STARTTIME parameter to specify when the initial startup window of the schedule starts.

You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

STARTTime

Specifies the time for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current time. This parameter is used in conjunction with the STARTDATE parameter to specify when the initial startup window begins.

You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW

Value	Description	Example
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with STARTTIME=NOW+02:00 or STARTTIME=+02:00, the beginning of the startup window is at 7:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW-02:00 **or** -02:00. If you issue this command at 5:00 with STARTTIME=NOW-02:00 or STARTTIME=-02:00, the beginning of the startup window is at 3:00.

DURation

Specifies the number of units that define the length of the startup window of the scheduled operation. This parameter is optional. This value must be from 1 to 999. The default is 1.

Use this parameter with the DURUNITS parameter to specify the length of the startup window. For example, if you specify DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The default length of the startup window is 1 hour. The duration of the window must be shorter than the period between windows.

This value is ignored if you specify DURUNITS=INDEFINITE.

Tip: Define schedules with durations longer than 10 minutes. Doing this will give the IBM Spectrum Protect scheduler enough time to process the schedule and prompt the client.

DURUnits

Specifies the time units used to determine the duration of the window in which the schedule can start. This parameter is optional. The default is HOURS.

Use this parameter with the DURATION parameter to specify how long the startup window remains open to process the schedule. For example, if DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The schedule may not necessarily complete processing within this window. If the schedule needs to be retried for any reason, the retry attempts must begin before the startup window elapses, or the operation does not restart.

The default value for the length of the startup window is 1 hour. You can specify one of the following values:

Minutes
: Specifies that the duration of the window is defined in minutes.

Hours
: Specifies that the duration of the window is defined in hours.

Days
: Specifies that the duration of the window is defined in days.

INDefinite
: Specifies that the startup window of the scheduled operation has an indefinite duration. The schedule can run any time after the scheduled start time, until the schedule expires. You cannot specify DURUNITS=INDEFINITE, unless you specify PERUNITS=ONETIME. The INDEFINITE value is not allowed with enhanced schedules.

MAXRUNtime

Specifies the maximum run time, which is the number of minutes during which all client sessions that are started by the scheduled operation should be completed. If sessions are still running after the maximum run time, the server issues a warning message, but the sessions continue to run.
Tip: The maximum run time is calculated from the beginning of the startup window and not from the time that sessions start within the startup window.
Restrictions:

- The value of the parameter is not distributed to servers that are managed by an enterprise configuration manager.
- The value of the parameter is not exported by the EXPORT command.

The parameter is optional. You can specify a number in the range 0-1440. The default value is 0. A value of 0 means that the maximum run time is indefinite, and no warning message is issued. The maximum run time must be greater than the startup window duration, which is defined by the DURATION and DURUNITS parameters.

For example, if the start time of a scheduled operation is 9:00 PM, and the duration of the startup window is 2 hours, the startup window is 9:00 PM - 11:00 PM. If the maximum run time is 240 minutes, that is, 4 hours, all client sessions for this operation should be completed by 1:00 AM. If one or more sessions are still running after 1:00 AM, the server issues a warning message.

Tip: Alternatively, you can specify a *Run time alert* value of 1:00 AM in the IBM Spectrum Protect Operations Center.

SCHEDStyle

This parameter is optional. SCHEDSTYLE defines either the interval between times when a schedule can run, or the days on which it runs. The default is the classic syntax.

Possible values are:

Classic

The parameters for the Classic syntax are: PERIOD, PERUNITS, and DAYOFWEEK. You cannot use these parameters: MONTH, DAYOFMONTH, and WEEKOFMONTH.

Enhanced

The parameters for the Enhanced syntax are: MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK. You cannot use these parameters: PERIOD and PERUNITS.

PERiod

Specifies the length of time between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. You can specify an integer from 1 to 999. The default is 1.

Use this parameter with the PERUNITS parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every five days after the initial start date and start time. The period between startup windows must exceed the duration of each window. The default is 1 day.

This value is ignored if you specify PERUNITS=ONETIME.

PERUnits

Specifies the time units used to determine the period between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. The default is DAYS.

Use this parameter with the PERIOD parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every 5 days after the initial start date and start time. The default is 1 day. You can specify one of the following values:

Hours

Specifies that the time between startup windows is in hours.

Days

Specifies that the time between startup windows is in days.

Weeks

Specifies that the time between startup windows is in weeks.

Months

Specifies that the time between startup windows is in months.

When you specify PERUNITS=MONTHS, the scheduled operation will be processed each month on the same date. For example, if the start date for the scheduled operation is 02/04/1998, the schedule will process on the 4th of every month thereafter. However, if the date is not valid for the next month, then the scheduled operation will be processed on the last valid date in the month. Thereafter, subsequent operations are based on this new date. For example, if the start date is 03/31/1998, the next month's operation will be scheduled for 04/30/1998. Thereafter, all subsequent operations will be on the 30th of the month until February. Because February has only 28 days, the operation will be scheduled for 02/28/1999. Subsequent operations will be processed on the 28th of the month.

Years

Specifies that the time between startup windows for the schedule is in years.

When you specify PERUNITS=YEARS, the scheduled operation will be processed on the same month and date of each year. For example, if the start date for the scheduled operation is 02/29/2004, the next year's scheduled operation will be 02/28/2005 because February only has 28 days. Thereafter, subsequent operations will be scheduled for February 28th.

Onetime

Specifies that the schedule processes once. This value overrides the value you specified for the PERIOD parameter.

DAYofweek

Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can specify different options for the DAYofweek parameter, depending on whether the schedule style was defined as Classic or Enhanced:

Classic Schedule

Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can either specify one day of the week, or WEEKDAY, WEEKEND, or ANY. If the start date and start time fall on a day that does not correspond to a day you specify, the start date and start time will be shifted forward in 24-hour increments until the DAYOFWEEK parameter is satisfied.

If you select a value for DAYOFWEEK other than ANY, and depending on the values for PERIOD and PERUNITS, schedules may not be processed when you would expect. The default is ANY.

Enhanced Schedule

Specifies the days of the week on which to run the schedule. You can either specify multiple days separated by commas and no intervening blanks, or WEEKDAY, WEEKEND, or ANY. If you specify multiple days, the schedule will run on each of the specified days. If you specify WEEKDAY or WEEKEND, you must also specify either WEEKOFMONTH=FIRST or WEEKOFMONTH=LAST, and the schedule will run just once per month.

The default value is ANY, meaning the schedule will run every day of the week or on the day or days determined by other enhanced schedule parameters. DAYOFWEEK must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

Possible values for the DAYofweek parameter are:

ANY
: Specifies that the startup window can begin on any day of the week.

WEEKDay
: Specifies that the startup window can begin on Monday, Tuesday, Wednesday, Thursday, or Friday.

WEEKEnd
: Specifies that the startup window can begin on Saturday or Sunday.

SUnday
: Specifies that the startup window begins on Sunday.

Monday
: Specifies that the startup window begins on Monday.

TUesday
: Specifies that the startup window begins on Tuesday.

Wednesday
: Specifies that the startup window begins on Wednesday.

THursday
: Specifies that the startup window begins on Thursday.

Friday
: Specifies that the startup window begins on Friday.

SAturday
: Specifies that the startup window begins on Saturday.

MONth
: Specifies the months of the year during which to run the schedule. This parameter is used only with enhanced schedules. Specify multiple values by using commas and no intervening blanks. The default value is ANY, which means that the schedule runs during every month of the year.

DAYOFMonth
: Specifies the day of the month to run the schedule. This parameter is used only with enhanced schedules. You can either specify ANY or a number from -31 through 31, excluding zero. Negative values are a day from the end of the month, counting backwards. For example, the last day of the month is -1, the next-to-the-last day of the month is -2, and so on. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule runs on each of the specified days of the month. If multiple values resolve to the same day, the schedule runs only once that day.

  The default value is ANY. ANY means that the schedule runs on every day of the month or on the days determined by other enhanced schedule parameters. DAYOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFWEEK or WEEKOFMONTH parameters.

WEEKofmonth

Specifies the week of the month in which to run the schedule. This parameter is used only with enhanced schedules. A week is considered any seven-day period which does not start on a particular day of the week. You can specify FIRST, SECOND, THIRD, FOURTH, LAST, or ANY. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule runs during each of the specified weeks of the month. If multiple values resolve to the same week, the schedule runs only once during that week.

The default value is ANY. ANY means that the schedule runs during every week of the month or on the day or days determined by other enhanced schedule parameters. WEEKOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

EXPiration
Specifies the date after which this schedule is no longer used. This parameter is optional. The default is NEVER. You can specify one of the following values:

Never
Specifies that the schedule never expires.

expiration_date
Specifies the date on which this schedule expires, in MM/DD/YYYY format. If you specify an expiration date, the schedule expires at 23:59:59 on the date you specify.

Example: Define a schedule for a monthly incremental backup

Define a schedule named MONTHLY_BACKUP that initiates an incremental backup of all associated nodes. Specify the start date as Tuesday, May 1, 2001. This date does not match the specified day of the week (Sunday), so the initial startup window begins on the first Sunday after May 1, 2001 (05/01/2001). The startup windows for this schedule extend from 01:00 through 03:00. This monthly schedule initiates backup of c: and d: file spaces for all associated nodes.

```
define schedule standard monthly_backup
description="Monthly Backup of c: and d: drives"
objects="c:\* d:\*"
startdate=05/01/2001 starttime=01:00
duration=2 durunits=hours period=1
perunits=months dayofweek=sunday
```

Example: Define a schedule for a weekly incremental backup

Define a schedule named WEEKLY_BACKUP that initiates an incremental backup of all associated nodes. The initial startup window for this schedule extends from 23:00 on Saturday, June 7, 1997 (06/07/1997), to 03:00 on Sunday, June 8, 1997 (06/08/1997). Subsequent windows begin at 23:00, every Saturday. No messages are returned to the client node when this schedule is run.

```
define schedule employee_records weekly_backup
startdate=06/07/1997 starttime=23:00 duration=4
durunits=hours perunits=weeks
dayofweek=saturday options=-quiet
```

Example: Define a schedule that archives a specific directory every quarter

Define a schedule that archives specific files quarterly on the last Friday of the month.

```
define schedule employee_records quarterly_archive
starttime=20:00 action=archive
object=/home/employee/records/*
duration=1 durunits=hour schedstyle=enhanced
month=mar,jun,sep,dec weekofmonth=last dayofweek=fri
```

DEFINE SCHEDULE (Define a schedule for an administrative command)

Use the DEFINE SCHEDULE command to create a new schedule for processing an administrative command.

You can include scripts in an administrative command schedule so the commands are processed automatically.
Note:

1. You cannot schedule the MACRO command or the QUERY ACTLOG command.

2. If you are scheduling a command that specifies the WAIT parameter, the parameter must be set to YES in order for the process to provide a return code to the session that started it. For more information about the WAIT parameter, see Server command processing.

Privilege class

To define an administrative command schedule, you must have system privilege.

Syntax

```
Classic administrative schedule

>>-DEFine SCHedule--schedule_name------------------------------>

>--+-------------------------+--CMD--=--command------------------>
   '-Type--=--Administrative-'

   .-ACTIVE--=--No--.
>--+----------------+--+----------------------------+---------->
   '-ACTIVE--=--Yes-'  '-DESCription--=--description-'

   .-PRIority--=--5------.  .-STARTDate--=--current_date-.
>--+--------------------+--+----------------------------+------>
   '-PRIority--=--number-'  '-STARTDate--=--date---------'

   .-STARTTime--=--current_time-.  .-DURation--=--1------.
>--+----------------------------+--+--------------------+------>
   '-STARTTime--=--time---------'  '-DURation--=--number-'

   .-DURUnits--=--Hours----------.  .-MAXRUNtime--=--0------.
>--+-----------------------------+--+----------------------+--->
   '-DURUnits--=--+-Minutes----+-'  '-MAXRUNtime--=--number-'
                  +-Hours------+
                  +-Days-------+
                  '-INDefinite-'

   .-SCHEDStyle--=--Classic-.  .-PERiod--=--1------.
>--+------------------------+--+------------------+------------>
   '-SCHEDStyle--=--Classic-'  '-PERiod--=--number-'

   .-PERUnits--=--Days--------.
>--+-------------------------+-------------------------------->
   '-PERUnits--=--+-Hours---+-'
                  +-Days----+
                  +-Weeks---+
                  +-Months--+
                  +-Years---+
                  '-Onetime-'

   .-DAYofweek--=--ANY-----------.
>--+-----------------------------+------------------------------>
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

   .-EXPiration--=--Never-----.
>--+-------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-date--'
```

Syntax

Enhanced administrative schedule

Parameters

schedule_name (Required)

Specifies the name of the schedule to be defined. You can specify up to 30 characters for the name.

Type=Administrative

Specifies that a schedule for an administrative command is defined. This parameter is optional. An administrative command is assumed if the CMD parameter is specified.

CMD (Required)

Specifies the administrative command to schedule for processing. The maximum length of the command is 512 characters. Enclose the administrative command in quotation marks if it contains any blank characters.

Restriction: You cannot specify redirection characters with this parameter.

ACTIVE

Specifies whether IBM Spectrum Protect processes an administrative command schedule when the startup window occurs. This parameter is optional. The default is NO. The administrative command schedule must be set to the active state with the UPDATE SCHEDULE command so that IBM Spectrum Protect can process the schedule. Possible values are:

YES

Specifies that IBM Spectrum Protect processes an administrative command schedule when the startup window begins.

NO

Specifies that IBM Spectrum Protect does not process an administrative command schedule when the startup window begins.

DESCription

Specifies a description of the schedule. This parameter is optional. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains any blank characters.

PRIority

Specifies the priority value for a schedule. This parameter is optional. You can specify an integer from 1 to 10, with 1 being the highest priority and 10 being the lowest. The default is 5.

If two or more schedules have the same window start time, the value you specify determines when IBM Spectrum Protect processes the schedule. The schedule with the highest priority starts first. For example, a schedule with PRIORITY=3 starts before a schedule with PRIORITY=5.

STARTDate

Specifies the date for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current date. Use this parameter with the STARTTIME parameter to specify when the initial startup window of the schedule starts.

You can specify the date using one of the values below:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

STARTTime

Specifies the time for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current time. This parameter is used in conjunction with the STARTDATE parameter to specify when the initial startup window begins.

You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with STARTTIME=NOW+02:00 or STARTTIME=+02:00, the beginning of the startup window is at 7:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW-02:00 **or** -02:00. If you issue this command at 5:00 with STARTTIME=NOW-02:00 or STARTTIME=-02:00, the beginning of the startup window is at 3:00.

DURation
Specifies the number of units that define the length of the startup window of the scheduled operation. This parameter is optional. This value must be from 1 to 999. The default is 1.

Use this parameter with the DURUNITS parameter to specify the length of the startup window. For example, if you specify DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The default length of the startup window is 1 hour. The duration of the window must be shorter than the period between windows.

This value is ignored if you specify DURUNITS=INDEFINITE.

DURUnits
Specifies the time units used to determine the duration of the window in which the schedule can start. This parameter is optional. The default is HOURS.

Use this parameter with the DURATION parameter to specify how long the startup window remains open to process the schedule. For example, if DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The schedule may not necessarily complete processing within this window. If the schedule needs to be retried for any reason, the retry attempts must begin before the startup window elapses, or the operation does not restart.

The default value for the length of the startup window is 1 hour. You can specify one of the following values:

Minutes
Specifies that the duration of the window is defined in minutes.
Hours
Specifies that the duration of the window is defined in hours.
Days
Specifies that the duration of the window is defined in days.
INDefinite
Specifies that the startup window of the scheduled operation has an indefinite duration. The schedule can run any time after the scheduled start time, until the schedule expires. You cannot specify DURUNITS=INDEFINITE, unless you specify PERUNITS=ONETIME. The INDEFINITE value is not allowed with enhanced schedules.

MAXRUNtime
Specifies the maximum run time, which is the number of minutes during which server processes that are started by the scheduled commands must be completed. If processes are still running after the maximum run time, the central scheduler cancels the processes.
Tips:

- The processes might not end immediately when the central scheduler cancels them; they end when they register the cancellation notification from the central scheduler.
- The maximum run time is calculated beginning from when the server process starts. If the schedule command starts more than one process, each process maximum run time is calculated from when the process starts.
- This parameter does not apply to some processes, such as duplicate-identification processes, which can continue to run after the maximum run time.
- This parameter does not apply if the scheduled command does not start a server process.
- Another cancel time might be associated with some commands. For example, the MIGRATE STGPOOL command can include a parameter that specifies the length of time that the storage pool migration runs before the migration is

automatically canceled. If you schedule a command for which a cancel time is defined, and you also define a maximum run time for the schedule, the processes are canceled at whichever cancel time is reached first.

Restrictions:

- The value of the parameter is not distributed to servers that are managed by an enterprise configuration manager.
- The value of the parameter is not exported by the EXPORT command.

The parameter is optional. You can specify a number in the range 0-1440. The default value is 0. A value of 0 means that the maximum run time is indefinite, and the central scheduler does not cancel processes. The maximum run time must be greater than the startup window duration, which is defined by the DURATION and DURUNITS parameters.

For example, if the start time of a scheduled command is 9:00 PM, and the duration of the startup window is 2 hours, the startup window is 9:00 PM - 11:00 PM. If the maximum run time is 240 minutes, that is, 4 hours, all applicable server processes that are started by the command must be completed by 1:00 AM. If one or more applicable processes are still running after 1:00 AM, the central scheduler cancels the processes.
Tip: Alternatively, you can specify an *end time* of 1:00 AM in the IBM Spectrum Protect Operations Center.

SCHEDStyle
: This parameter is optional. SCHEDSTYLE defines either the interval between times when a schedule should run, or the days on which it should run. The style can be either classic or enhanced. The default is the classic syntax.

  For classic schedules, these parameters are allowed: PERIOD, PERUNITS, and DAYOFWEEK. Not allowed for classic schedules are: MONTH, DAYOFMONTH, and WEEKOFMONTH.

  For enhanced schedules, these parameters are allowed: MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK. These parameters are not allowed: PERIOD and PERUNITS.

PERiod
: Specifies the length of time between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. You can specify an integer from 1 to 999. The default is 1.

  Use this parameter with the PERUNITS parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every five days after the initial start date and start time. The period between startup windows must exceed the duration of each window. The default is 1 day.

  This value is ignored if you specify PERUNITS=ONETIME.

PERUnits
: Specifies the time units used to determine the period between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. The default is DAYS.
  Use this parameter with the PERIOD parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every 5 days after the initial start date and start time. The default is 1 day. You can specify one of the following values:

  Hours
  : Specifies that the time between startup windows is in hours.

  Days
  : Specifies that the time between startup windows is in days.

  Weeks
  : Specifies that the time between startup windows is in weeks.

  Months
  : Specifies that the time between startup windows is in months.

    When you specify PERUNITS=MONTHS, the scheduled operation will be processed each month on the same date. For example, if the start date for the scheduled operation is 02/04/1998, the schedule will process on the 4th of every month thereafter. However, if the date is not valid for the next month, then the scheduled operation will be processed on the last valid date in the month. Thereafter, subsequent operations are based on this new date. For example, if the start date is 03/31/1998, the next month's operation will be scheduled for 04/30/1998. Thereafter, all subsequent operations will be on the 30th of the month until February. Because February has only 28 days, the operation will be scheduled for 02/28/1999. Subsequent operations will be processed on the 28th of the month.

  Years
  : Specifies that the time between startup windows for the schedule is in years.

When you specify PERUNITS=YEARS, the scheduled operation will be processed on the same month and date of each year. For example, if the start date for the scheduled operation is 02/29/2004, the next year's scheduled operation will be 02/28/2005 because February only has 28 days. Thereafter, subsequent operations will be scheduled for February 28th.

Onetime
Specifies that the schedule processes once. This value overrides the value you specified for the PERIOD parameter.

DAYofweek
Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can specify different options for the DAYofweek parameter, depending on whether the schedule style was defined as Classic or Enhanced:

Classic Schedule
Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can either specify one day of the week, or WEEKDAY, WEEKEND, or ANY. If the start date and start time fall on a day that does not correspond to a day you specify, the start date and start time will be shifted forward in 24-hour increments until the DAYOFWEEK parameter is satisfied.

If you select a value for DAYOFWEEK other than ANY, and depending on the values for PERIOD and PERUNITS, schedules may not be processed when you would expect. The default is ANY.

Enhanced Schedule
Specifies the days of the week on which to run the schedule. You can either specify multiple days separated by commas and no intervening blanks, or WEEKDAY, WEEKEND, or ANY. If you specify multiple days, the schedule will run on each of the specified days. If you specify WEEKDAY or WEEKEND, you must also specify either WEEKOFMONTH=FIRST or WEEKOFMONTH=LAST, and the schedule will run just once per month.

The default value is ANY, meaning the schedule will run every day of the week or on the day or days determined by other enhanced schedule parameters. DAYOFWEEK must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

Possible values for the DAYofweek parameter are:

ANY
Specifies that the startup window can begin on any day of the week.
WEEKDay
Specifies that the startup window can begin on Monday, Tuesday, Wednesday, Thursday, or Friday.
WEEKEnd
Specifies that the startup window can begin on Saturday or Sunday.
SUnday
Specifies that the startup window begins on Sunday.
Monday
Specifies that the startup window begins on Monday.
TUesday
Specifies that the startup window begins on Tuesday.
Wednesday
Specifies that the startup window begins on Wednesday.
THursday
Specifies that the startup window begins on Thursday.
Friday
Specifies that the startup window begins on Friday.
SAturday
Specifies that the startup window begins on Saturday.

MONth
Specifies the months of the year during which to run the schedule. This parameter is used only with enhanced schedules. Specify multiple values by using commas and no intervening blanks. The default value is ANY. This means the schedule will run during every month of the year.

DAYOFMonth
Specifies the day of the month to run the schedule. This parameter is used only with enhanced schedules. You can either specify ANY or a number from -31 through 31, excluding zero. Negative values are a day from the end of the month, counting backwards. For example, the last day of the month is -1, the next-to-the-last day of the month is -2, etc. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule will

run on each of the specified days of the month. If multiple values resolve to the same day, the schedule will run only once that day.

The default value is ANY This means the schedule will run on every day of the month or on the days determined by other enhanced schedule parameters. DAYOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFWEEK or WEEKOFMONTH parameters.

WEEKofmonth
Specifies the week of the month in which to run the schedule. This parameter is used only with enhanced schedules. A week is considered any seven-day period which does not start on a particular day of the week. You can specify FIRST, SECOND, THIRD, FOURTH, LAST, or ANY. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule will run during each of the specified weeks of the month. If multiple values resolve to the same week, the schedule will run only once during that week.

The default value is ANY, meaning the schedule will run during every week of the month or on the day or days determined by other enhanced schedule parameters. WEEKOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

EXPiration
Specifies the date after which this schedule is no longer used. This parameter is optional. The default is NEVER. You can specify one of the following values:

Never
Specifies that the schedule never expires.

expiration_date
Specifies the date on which this schedule expires, in MM/DD/YYYY format. If you specify an expiration date, the schedule expires at 23:59:59 on the date you specify.

Example: Define a schedule to back up the primary storage pool every two days

Define a schedule named BACKUP_ARCHIVEPOOL that backs up the primary storage pool ARCHIVEPOOL to the copy storage pool RECOVERYPOOL. The backup runs at 8 p.m. every two days.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
active=yes starttime=20:00 period=2
```

Example: Define a schedule to back up the primary storage pool twice a month

Define a schedule named BACKUP_ARCHIVEPOOL that backs up the primary storage pool ARCHIVEPOOL to the copy storage pool RECOVERYPOOL. Select an enhanced schedule and run on the first and fifteenth day of the month.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
schedstyle=enhanced dayofmonth=1,15
```

DEFINE SCRATCHPADENTRY (Define a scratch pad entry)

Use this command to enter data on a new line in the scratch pad. The scratch pad is a database table that the server hosts. You can use the scratch pad to store diverse information in table format.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine SCRATCHPadentry--major_category--minor_category------->

>--subject--Line--=--number--Data--=--data--------------------><
```

Parameters

major_category (Required)
: Specifies the major category in which data is to be stored. Enter a text string of up to 100 alphanumeric characters. This parameter is case sensitive.

minor_category (Required)
: Specifies the minor category in which data is to be stored. Minor categories are sections within major categories. Enter a text string of up to 100 alphanumeric characters. This parameter is case sensitive.

subject (Required)
: Specifies the subject under which data is to be stored. Subjects are sections within minor categories. Enter a text string of up to 100 alphanumeric characters. This parameter is case sensitive.

Line (Required)
: Specifies the number of the line on which data is to be stored. Lines are sections within subjects. Specify an integer in the range 1 - 1000.

Data (Required)
: Specifies the data to be stored on the line. You can enter up to 1000 characters. Enclose the data in quotation marks if the data contains one or more blanks. The data is case sensitive.

Example: Define a scratch pad entry

Enter the vacation dates of an administrator, Jane, in a table that stores information about the location of all administrators.

```
define scratchpadentry admin_info location jane line=2 data=
"Out of the office from 1-15 Nov."
```

Related commands

Table 1. Commands related to DEFINE SCRATCHPADENTRY

Command	Description
DELETE SCRATCHPADENTRY	Deletes a line of data from the scratch pad.
QUERY SCRATCHPADENTRY	Displays information that is contained in the scratch pad.
SET SCRATCHPADRETENTION	Specifies the amount of time for which scratch pad entries are retained.
UPDATE SCRATCHPADENTRY	Updates data on a line in the scratch pad.

DEFINE SCRIPT (Define an IBM Spectrum Protect script)

Use this command to define an IBM Spectrum Protect™ script or to create a new IBM Spectrum Protect script by using the contents from another script.

The first line for the script can be defined with this command. To add subsequent lines to the script, use the UPDATE SCRIPT command.

Tips:

- When routing commands inside scripts, enclose the server or server group in parentheses and omit the colon. Otherwise, if the syntax includes a colon, the command is not routed when the RUN command is issued. Instead, the command runs only on the server from which the RUN command is issued.
- You cannot redirect the output of a command within an IBM Spectrum Protect script. Instead, run the script and then specify command redirection. For example, to direct the output of script1 to the c:\temp\test.out directory, run the script and specify command redirection as in the following example:

  ```
  run script1 > c:\temp\test.out
  ```

Privilege class

To issue this command, you must have operator, policy, storage, or system privilege.

Syntax

```
>>-DEFine SCRipt--script_name-------------------------------------->
```

```
                  .-Line--=--001----.
>--+-command_line--+-----------------+-+----------------------->
   |               '-Line -=--number-' |
   '-File--=--file_name----------------'

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

script_name (Required)
: Specifies the name of the script to be defined. You can specify up to 30 characters for the name.

command_line
: Specifies the first command to be processed in a script. You must specify either this parameter (and optionally, the LINE parameter) or the FILE parameter.

  The command that you specify can include substitution variables and can be continued across multiple lines if you specify a continuation character (-) as the last character in the command. Substitution variables are specified with a '$' character, followed by a number that indicates the value of the parameter when the script is processed. You can specify up to 1200 characters for the command line. Enclose the command in quotation marks if it contains blanks.

  You can run commands serially, in parallel, or serially and in parallel by specifying the SERIAL or PARALLEL script commands for the COMMAND_LINE parameter. You can run multiple commands in parallel and wait for them to complete before you proceed to the next command. Commands run serially until the parallel command is encountered.

  Conditional logic flow statements can be used. These statements include IF, EXIT, and GOTO.

  Line
  : Specifies the line number for the command line. Because commands are specified in multiple lines, line numbers are used to determine the order for processing when the script is run. The first line, or line 001 is the default. This parameter is optional.

File
: Specifies the name of the file whose contents are read into the script to be defined. The file must reside on the server where this command is running. If you specify the FILE parameter, you cannot specify a command line or line number.

  You can create a script by querying another script and specifying the FORMAT=RAW and OUTPUTFILE parameters. The output from querying the script is directed to a file you specify with the OUTPUTFILE parameter. To create the new script, the contents of the script to be defined are read in from the file you specified with the OUTPUTFILE parameter.

DESCription
: Specifies a description for the script. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains blank characters. This parameter is optional.

Example: Write a script to display AIX clients

Define a script that displays all AIX® clients.

```
define script qaixc "select node_name from nodes where platform_name='AIX'"
  desc='Display aix clients'
```

Example: Write and run a script to route a command to a server group

Define and run a script that routes the QUERY STGPOOL command to a server group named DEV_GROUP.

```
define script qu_stg "(dev_group) query stgpool"

run qu_stg
```

Example: Create a script from an existing script

Define a script whose command lines are read in from a file that is named MY.SCRIPT and name the new script AGADM. The file must be on the server, and be read by the server.

```
define script agadm file=my.script
```

Related commands

Table 1. Commands related to DEFINE SCRIPT

Command	Description
COPY SCRIPT	Creates a copy of a script.
DELETE SCRIPT	Deletes the script or individual lines from the script.
QUERY SCRIPT	Displays information about scripts.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

Related concepts:
Using logic flow statements in a script
Related tasks:
Defining a server script
Running commands in parallel or serially
Performing tasks concurrently on multiple servers
Related reference:
Return codes for use in IBM Spectrum Protect scripts

DEFINE SERVER (Define a server for server-to-server communications)

Use this command to define a server to use functions such as virtual volumes, node replication, command routing, and LAN-free data movement, among others.

Use this command to define a server for the following functions:

- Enterprise configuration
- Enterprise event logging
- Command routing
- Virtual volumes
- LAN-free data movement
- Node replication
- AIX Linux Data movement by using z/OS® media server
- Status monitoring of remote servers
- Alert monitoring of remote servers
- Server-to-server export

If you use an LDAP directory server to authenticate passwords, any target servers must be configured for LDAP-authenticated passwords. Data that is replicated from a node that authenticates with an LDAP directory server is inaccessible if the target replication server is not properly configured. If your target replication server is not configured, replicated data from an LDAP node can make it to the target server. But the target replication server must be configured to use LDAP if you want to access the data.

The use of virtual volumes is not supported when the source server and the target server are on the same IBM Spectrum Protect™ server.

This command also is used to define an IBM Spectrum Protect storage agent as if it were a server.

Privilege class

To issue this command, you must have system privilege.

Syntax

For:

- Command routing
- Status monitoring of remote servers

- Alert monitoring of remote servers
- Server-to-server export

Tip: Command routing uses the ID and the password of the administrator who is issuing the command.

```
>>-DEFine--SERver--server_name--HLAddress--=--ip_address-------->

>--LLAddress--=--tcp_port--+---------------------+------------->
                           '-COMMmethod--=--TCPIP-'

>--+-------------+--+----------------------------+------------->
   '-URL--=--url-'  '-DESCription--=--description-'

   .-SSL--=--No------.
>--+-----------------+------------------------------------------>
   '-SSL--=--+-No--+-'
             '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-------------------------------------+-------------------><
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'
```

Syntax

For:

- Enterprise configuration
- Enterprise event logging
- Storage agent
- Node replication source and target servers
- AIX Linux z/OS media server

```
>>-DEFine--SERver--server_name--SERVERPAssword--=--password----->

>--HLAddress--=--ip_address--LLAddress--=--tcp_port------------->

>--+---------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--url-'

>--+-----------------------------+------------------------------>
   '-DESCription--=--description-'

                          (1)
   .-CROSSDEFine--=--No-------. (2)
>--+-------------------------+-------------------------------->
   '-CROSSDEFine--=--+-No--+--'
                     '-Yes-'

   .-VALIdateprotocol--=--No------.  .-SSL--=--No------.
>--+-----------------------------+--+-----------------+-------->
   '-VALIdateprotocol--=--+-No--+-'  '-SSL--=--+-No--+-'
                          '-All-'              '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-------------------------------------+-------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------+------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (3) |
                        '-Fasp-----'
```

Notes:

1. The CROSSDEFINE parameter does not apply to storage agent definitions.

2. The VALIDATEPROTOCOL parameter is deprecated and applies only to storage agent definitions.
3. Linux The TRANSFERMETHOD parameter is available only on Linux x86_64 operating systems.

Syntax for virtual volumes

```
>>-DEFine--SERver--server_name--PAssword--=--password----------->

>--HLAddress--=--ip_address--LLAddress--=--tcp_port------------->

>--+----------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--url-'

>--+-------------------------+--+-----------------------+------>
   '-DELgraceperiod--=--days-'  '-NODEName--=--node_name-'

                                  .-SSL--=--No------.
>--+-----------------------------+--+-----------------+--------->
   '-DESCription--=--description-'  '-SSL--=--+-No--+-'
                                              '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+--------------------------------------+-------------------><
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'
```

Parameters

server_name (Required)
: Specifies the name of the server. This name must be unique on the server. The maximum length of this name is 64 characters.

  For server-to-server event logging, library sharing, and node replication, you must specify a server name that matches the name that was set by issuing the SET SERVERNAME command at the target server.

PAssword
: Specifies the password that is used to sign on to the target server for virtual volumes. If you specify the NODENAME parameter, you must specify the PASSWORD parameter. If you specify the PASSWORD parameter but not the NODENAME parameter, the node name defaults to the server name that is specified with the SET SERVERNAME command. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

SERVERPAssword
: Specifies the password of the server that you are defining. This password must match the password that is set by the SET SERVERPASSWORD command. This parameter is required for enterprise configuration and server-to-server event logging functions. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

HLAddress (Required)
: Specifies the IP address (in dotted decimal format) of the server.

  Do not use the loopback address as the value of this parameter. Virtual volumes are not supported when the source server and the target server are the same IBM Spectrum Protect server.

LLAddress (Required)
: Specifies the low-level address of the server. This address is usually the same as the address in the TCPPORT server option of the target server. When SSL=YES, the port must already be designated for SSL communications on the target server.

COMMmethod
: Specifies the communication method that is used to connect to the server. This parameter is optional.

URL
: Specifies the URL address of this server. The parameter is optional.

DELgraceperiod
: Specifies a number of days that an object remains on the target server after it was marked for deletion. You can specify a value 0 - 9999. The default is 5. This parameter is optional.

NODEName
: Specifies a node name to be used by the server to connect to the target server. This parameter is optional. If you specify the NODENAME parameter, you must also specify the PASSWORD parameter. If you specify the PASSWORD parameter but not

the NODENAME parameter, the node name defaults to the server name specified with the SET SERVERNAME command.

DESCription

Specifies a description of the server. The parameter is optional. The description can be up to 255 characters. Enclose the description in quotation marks if it contains blank characters.

CROSSDEFine

Specifies whether the server that is running this command defines itself to the server that is being specified by this command. This parameter is optional.

AIX | Linux | Windows Important: This parameter does not apply to storage agent definitions.

If this parameter is included, you must also issue the SET SERVERNAME, SET SERVERPASSWORD, SET SERVERHLADDRESS, SET CROSSDEFINE, and SET SERVERLLADDRESS commands. The default is NO.

Remember:

- For replication operations, the names of the source and target replication servers must match the names that you specify in this command.
- CROSSDEFINE can be used with SSL=YES if all of the conditions that are specified for the SSL=YES parameter are in place on the source and target server.

You can specify one of the following values:

No

Cross definition is not completed.

Yes

Cross definition is completed.

VALIdateprotocol (deprecated)

Specifies whether a cyclic redundancy check validates the data that is sent between the storage agent and IBM Spectrum Protect server. The parameter is optional. The default is NO.

Important: Beginning with IBM Spectrum Protect Version 8.1.2 and Tivoli® Storage Manager Version 7.1.8, validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The VALIDATEPROTOCOL parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

SSL

Specifies the communication mode of the server. The default is NO.

Important: Beginning in IBM Spectrum Protect V8.1.2 and Tivoli Storage Manager V7.1.8, the SSL parameter uses SSL to encrypt some communication with the specified server even if SSL=NO.

The following conditions and considerations apply when you specify the SSL parameter:

- Before you start the servers, self-signed certificates of the partner servers must be in the key database file (cert.kdb) of each of the servers.
- You can define multiple server names with different parameters for the same target server.
- Storage agents can issue the DSMSTA SETSTORAGESERVER command and include the SSL parameter to create the key database.

You can specify one of the following values:

No

Specifies an SSL session for all communication with the specified server, except when the server is sending or receiving object data. Object data is sent and received by using TCP/IP. By choosing not to encrypt the object data, server performance is similar to communication over a TCP/IP session and the session is secure.

Yes

Specifies an SSL session for all communication with the specified server, even when the server is sending and receiving object data.

SESSIONSECurity

Specifies whether the server that you are defining must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

You can specify one of the following values:

STRict

Specifies that the strictest security settings are enforced for the server that you are defining. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the specified server and an IBM Spectrum Protect server.

To use the STRICT value, the following requirements must be met to ensure that the specified server can authenticate with the IBM Spectrum Protect server:

- Both the server that you are defining and the IBM Spectrum Protect server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
- The server that you are defining must be configured to use the TLS 1.2 protocol for SSL sessions between itself and the IBM Spectrum Protect server.

Servers set to STRICT that do not meet these requirements are unable to authenticate with the IBM Spectrum Protect server.

TRANSitional

Specifies that the existing security settings are enforced for the server. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the server has never met the requirements for the STRICT value, the server will continue to authenticate by using the TRANSITIONAL value. However, after a server meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the server can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after a server successfully authenticates by using a more secure communication protocol, the server can no longer authenticate by using a less secure protocol. For example, if a server that is not using SSL is updated and successfully authenticates by using TLS 1.2, the server can no longer authenticate by using no SSL protocol or TLS 1.1. This restriction also applies when you use functions such as virtual volumes, command routing, or server-to-server export, when a node or administrator authenticates to the IBM Spectrum Protect server as a node or administrator from another server.

Linux TRANSFERMethod

Linux Specifies the method that is used for server-to-server data transfer. This parameter is optional. You can specify one of the following values:

Tcpip

Specifies that TCP/IP is used to transfer data. This is the default.

Fasp

Specifies that Aspera® Fast Adaptive Secure Protocol (FASP®) technology is used to transfer data. Aspera FASP technology can help you optimize data transfer in a wide area network (WAN).
Restrictions:

- Before you enable Aspera FASP technology, determine whether the technology is appropriate for your system environment and install the appropriate licenses. For instructions, see Determining whether Aspera FASP technology can optimize data transfer in your system environment. If the licenses are missing or expired, data transfer operations fail.
- If WAN performance meets your business needs, do not enable Aspera FASP technology.
- If you specify TRANSFERMETHOD=FASP on the PROTECT STGPOOL or REPLICATE NODE command, that value overrides the TRANSFERMETHOD parameter on the DEFINE SERVER and UPDATE SERVER commands.

Example: Set up two servers to use SSL to communicate (manual configuration)

Tip: If both servers are using IBM Spectrum Protect V8.1.2 or later software or Tivoli Storage Manager V7.1.8 software, SSL is automatically configured between the servers and manual configuration is not required.
If both servers are not using V7.1.8 or V8.1.2 or later software, you must manually configure the two servers to use SSL to communicate.
The server addresses are as follows:

- ServerA is at `bfa.tucson.ibm.com`
- ServerB is at `bfb.tucson.ibm.com`

Complete the following steps to set up the two servers for SSL:

1. Specify option TCPPORT 1500 for both servers in the dsmserv.opt option file.
2. Start both servers.
3. Shut down both servers to import the cert256 partner certificate. For ServerA, the certificate is in the /tsma instance directory. For ServerB, the certificate is in the /tsmb instance directory.
4. Start both servers. The /tsma/cert256.arm file is copied to /tsmb/cert256.bfa.arm on the bfb.tucson.ibm.com address. The /tsmb/cert256.arm file is copied to /tsmb/cert256.bfb.arm on the bfa.tucson.ibm.com address.

5. Issue the following command:
   - From ServerA:

     ```
     gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
     -label "bfb" -file /tsma/cert256.bfb.arm
     ```

   - From ServerB:

     ```
     gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
     -label "bfa" -file /tsmb/cert256.bfa.arm
     ```

   From each server, you can view the certificates in the key database by issuing the following command:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

6. Restart the servers.
7. Issue the appropriate DEFINE SERVER command. For ServerA, issue the following example command:

   ```
   DEFINE SERVER BFB hla=bfb.tucson.ibm.com lla=1542
   serverpa=passwordforbfb SSL=YES
   ```

   For ServerB, issue the following example command:

   ```
   DEFINE SERVER BFA hla=bfa.tucson.ibm.com lla=1542
   serverpa=passwordforbfa SSL=YES
   ```

If you do not use SSL, issue the following example DEFINE SERVER command on ServerA:

```
DEFINE SERVER BFBTCP hla=bfb.tucson.ibm.com lla=1500
serverpa=passwordforbfb SSL=NO
```

If you do not use SSL, issue the following example DEFINE SERVER command on ServerB:

```
DEFINE SERVER BFATCP hla=bfa.tucson.ibm.com lla=1500
serverpa=passwordforbfa SSL=NO
```

Example: Define a server to communicate with another server by using strict session security

Define a server name of SERVER1 to use the strictest security settings to authenticate with the IBM Spectrum Protect server.

```
define server server1 sessionsecurity=strict
```

Example: Define a target server

A target server has a high-level address of 9.116.2.67 and a low-level address of 1570. Define that target server to the source server, name the target server SERVER2, and set the password to SECRETPASSWORD. Specify that objects remain on the target server for seven days after they are marked for deletion.

```
define server server2 password=secretpassword
  hladdress=9.116.2.67 lladdress=1570 delgraceperiod=7
```

Example: Define a server to receive commands from other servers

Define a server that can receive commands that are routed from other servers. Name the server WEST_COMPLEX. Set the high-level address to 9.172.12.35, the low-level address to 1500, and the URL address to http://west_complex:1580/.

```
define server west_complex
hladdress=9.172.12.35 lladdress=1500
url=http://west_complex:1580/
```

Example: Cross-define two servers

Use cross definition to define SERVER_A and SERVER_B.

1. On SERVER_B, specify the server name, password, and high- and low-level addresses of SERVER_B. Specify that cross defining is allowed.

   ```
   set servername server_b
   set serverpassword mylifepwd
   set serverhladdress 9.115.20.80
   ```

```
set serverlladdress 1860
set crossdefine on
```

2. On SERVER_A, specify the server name, password, and high- and low-level addresses of SERVER_A.

```
set servername server_a
set serverpassword yourlifepwd
set serverhladdress 9.115.20.97
set serverlladdress 1500
```

3. On SERVER_A, define SERVER_B:

```
define server server_b hladdress=9.115.20.80 lladdress=1860
serverpassword=mylifepwd crossdefine=yes
```

Related commands

Table 1. Commands related to DEFINE SERVER

Command	Description
DEFINE DEVCLASS	Defines a device class.
AIX Linux DEFINE PATH	AIX Linux Define a path when the destination is a z/OS media server.
DELETE DEVCLASS	Deletes a device class.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
DELETE SERVER	Deletes the definition of a server.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY SERVER	Displays information about servers.
RECONCILE VOLUMES	Reconciles source server virtual volume definitions and target server archive objects.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
SET CROSSDEFINE	Specifies whether to cross define servers.
SET SERVERNAME	Specifies the name by which the server is identified.
SET SERVERHLADDRESS	Specifies the high-level address of a server.
SET SERVERLLADDRESS	Specifies the low-level address of a server.
SET SERVERPASSWORD	Specifies the server password.
SET REPLSERVER	Specifies a target replication server.
UPDATE DEVCLASS	Changes the attributes of a device class.
UPDATE NODE	Changes the attributes that are associated with a client node.
AIX Linux UPDATE PATH	AIX Linux Define a path when the destination is a z/OS media server.
UPDATE SERVER	Updates information about a server.

DEFINE SERVERGROUP (Define a server group)

Use this command to define a server group. With a server group, you can route commands to multiple servers by specifying only the group name. After you define the server group, add servers to the group by using the DEFINE GRPMEMBER command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine SERVERGroup--group_name------------------------------>

>--+-----------------------------+---------------------------><
   '-DESCription--=--description-'
```

Parameters

group_name (Required)
: Specifies the name of the server group. The maximum length of the name is 64 characters.

DESCription
: Specifies a description of the server group. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Example: Define a server group

Define a server group named WEST_COMPLEX.

```
define servergroup west_complex
```

Related commands

Table 1. Commands related to DEFINE SERVERGROUP

Command	Description
COPY SERVERGROUP	Creates a copy of a server group.
DEFINE GRPMEMBER	Defines a server as a member of a server group.
DELETE GRPMEMBER	Deletes a server from a server group.
DELETE SERVERGROUP	Deletes a server group.
MOVE GRPMEMBER	Moves a server group member.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

DEFINE SPACETRIGGER (Define the space trigger)

Use this command to define settings for triggers that determine when and how the server prepares extra space when predetermined thresholds are exceeded in storage pools that use FILE and DISK device classes. Space triggers are not enabled for storage pools with a parameter RECLAMATIONTYPE=SNAPLOCK.

The IBM Spectrum Protect™ server allocates more space when space utilization reaches a specified value. After allocating more space, the server either adds the space to the specified pool (random-access or sequential-access disk).

Important: Space trigger functions and storage pool space calculations take into account the space remaining in each directory. An inaccurate calculation can result in a failure to expand the space available in a storage pool. Failure to expand space in a storage pool is one of the conditions that can cause a trigger to become disabled.

For example, if you specify multiple directories for a device class and the directories reside in the same file system, the server calculates space by adding values representing the space remaining in each directory. These space calculations are inaccurate. Rather than choosing a storage pool with sufficient space for an operation, the server might choose the directory that is specified for the device class and run out of space prematurely.

To prevent possible problems and ensure an accurate calculation, you associate each directory with a separate file system. If a trigger becomes disabled because the space in a storage pool could not be expanded, you can re-enable the trigger by specifying the following command: `update spacetrigger stg`. No further changes are required to the space trigger.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
                                .-Fullpct--=--80------.
>>-DEFine SPACETrigger----STG----+---------------------+-------->
                                '-Fullpct--=--percent-'

   .-SPACEexpansion--=--20------.
>--+----------------------------+------------------------------>
   '-SPACEexpansion--=--percent-'

>--+----------------------------+------------------------------>
   '-EXPansionprefix--=--prefix-'

>--+------------------------------+--------------------------><
   '-STGPOOL--=--storage_pool_name-'
```

Parameters

STG
: Specifies a storage pool space trigger.

Fullpct
: This parameter specifies the utilization percentage of the storage pool. This parameter is optional. Specify an integer value 0 - 99. The default is 80. A value of zero (0) disables the space trigger. When this value is exceeded, the space trigger creates new volumes. Exceeding the threshold might not cause new volumes to be created until the next space request is made.

  You can determine storage pool utilization by issuing the QUERY STGPOOL command with FORMAT=DETAILED. The percentage of storage pool utilization is displayed in the field "Space Trigger Util." The calculation for this percentage does not include potential scratch volumes. The calculation for the percentage utilization that is used for migration and reclamation, however, does include potential scratch volumes.

SPACEexpansion
: For sequential-access FILE-type storage pools, this parameter is used in determining the number of additional volumes that are created in the storage pool. This parameter is optional. The default is 20. Volumes are created using the MAXCAPACITY value from the storage pool's device class. For random-access DISK storage pools, the space trigger creates a single volume using the EXPANSIONPREFIX.

EXPansionprefix
: For random-access DISK storage-pools, this parameter specifies the prefix that the server uses to create new storage pool files. This parameter is optional and applies only to random-access DISK device classes. The default prefix is the server installation path.
  The prefix can include one or more directory separator characters, for example: AIX Linux

  ```
  /opt/tivoli/tsm/server/bin/
  ```

  Windows

  ```
  c:\program files\tivoli\tsm\
  ```

  AIX Linux You can specify up to 250 characters. If you specify an invalid prefix, automatic expansion can fail.

  Windows You can specify up to 200 characters. If you specify an invalid prefix, automatic expansion can fail. If the server is running as a Windows service, the default prefix is the c:\wnnt\system32 directory.

  This parameter is not valid for space triggers for sequential-access FILE storage pools. Prefixes are obtained from the directories that are specified with the associated device class.

STGPOOL

Specifies the storage pool that is associated with this space trigger. This parameter is optional for storage pool space triggers. If you specify the STG parameter but not the STGPOOL parameter, one space trigger is created that applies to all random-access DISK and sequential-access FILE storage pools that do not have a specific space trigger.

This parameter does not apply to storage pools with the parameter RECLAMATIONTYPE=SNAPLOCK.

Example: Define a space trigger to increase storage pool space 25 percent

Set up a storage pool space trigger for increasing the amount of space in a storage pool by 25 percent when it is filled to 80 percent utilization of existing volumes. Space is created in the directories associated with the device class.

```
define spacetrigger stg spaceexpansion=25 stgpool=file
```

Example: Define a space trigger to increase storage pool space 40 percent

Set up a space trigger for the WINPOOL1 storage pool to increase the amount of space in the storage pool by 40 percent when it is filled to 80 percent utilization of existing volumes.

```
define spacetrigger stg spaceexpansion=40 stgpool=winpool1
```

Related commands

Table 1. Commands related to DEFINE SPACETRIGGER

Command	Description
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE SPACETRIGGER	Deletes the storage pool space trigger.
QUERY SPACETRIGGER	Displays information about a storage pool space trigger.
UPDATE SPACETRIGGER	Changes attributes of storage pool space trigger.

DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)

Use this command to define a new status monitoring threshold.

Status monitoring thresholds compare the defined conditions to the status monitoring server queries and inserts the results in the status monitoring table.

Multiple thresholds can be defined for an activity. For example, you can create a threshold that provides a warning status if storage pool capacity utilization is greater than 80%. You can then create another threshold that provides error status if storage pool capacity utilization is greater than 90%.

Note: If a threshold is already defined for an EXISTS condition, you cannot define another threshold with one of the other condition types.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine STAtusthreshold--threshold_name--activity------------->

   .-Condition--=--EXists-----.
>--+--------------------------+--+-----------------+------------>
   '-Condition--=--+-EXists-+-'  '-Value--=--value-'
                   +-GT-----+
                   +-GE-----+
                   +-LT-----+
                   +-LE-----+
                   '-EQual--'
```

```
   .-STatus--=--Normal------.
>--+------------------------+---------------------------------><
   '-STatus--=--+-Normal--+-'
                +-Warning-+
                '-Error---'
```

Parameters

threshold_name (Required)
: Specifies the threshold name. The name cannot exceed 48 characters in length.

activity (Required)
: Specifies the activity for which you want to create status indicators. Specify one of the following values:

PROCESSSUMMARY
: Specifies the number of processes that are currently active.

SESSIONSUMMARY
: Specifies the number of sessions that are currently active.

CLIENTSESSIONSUMMARY
: Specifies the number of client sessions that are currently active.

SCHEDCLIENTSESSIONSUMMARY
: Specifies the number of scheduled client sessions.

DBUTIL
: Specifies the database utilization percentage. The default warning threshold value is 80%, and the default error threshold value is 90%.

DBFREESPACE
: Specifies the free space available in the database in gigabytes.

DBUSEDSPACE
: Specifies the amount of database space that is used, in gigabytes.

ARCHIVELOGFREESPACE
: Specifies the free space that is available in the archive log, in gigabytes.

STGPOOLUTIL
: Specifies the storage pool utilization percentage. The default warning threshold value is 80%, and the default error threshold value is 90%.

STGPOOLCAPACITY
: Specifies the storage pool capacity in gigabytes.

AVGSTGPOOLUTIL
: Specifies the average storage pool utilization percentage across all storage pools. The default warning threshold value is 80%, and the default error threshold value is 90%.

TOTSTGPOOLCAPACITY
: Specifies the total storage pool capacity in gigabytes for all available storage pools.

TOTSTGPOOLS
: Specifies the number of defined storage pools.

TOTRWSTGPOOLS
: Specifies the number of defined storage pools that are readable or writeable.

TOTNOTRWSTGPOOLS
: Specifies the number of defined storage pools that are not readable or writeable.

STGPOOLINUSEANDDEFINED
: Specifies the total number of defined volumes that are in use.

ACTIVELOGUTIL
: Specifies the current percent utilization of the active log. The default warning threshold value is 80%, and the default error threshold value is 90%.

ARCHLOGUTIL
: Specifies the current utilization of the archive log. The default warning threshold value is 80%, and the default error threshold value is 90%.

CPYSTGPOOLUTIL
: Specifies the percent utilization for a copy storage pool. The default warning threshold value is 80%, and the default error threshold value is 90%.

PMRYSTGPOOLUTIL
: Specifies the percent utilization for a primary storage pool. The default warning threshold value is 80%, and the default error threshold value is 90%.

DEVCLASSPCTDRVOFFLINE

Specifies the percent utilization of drives that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDRVPOLLING
: Specifies the drives polling, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTLIBPATHSOFFLINE
: Specifies the library paths that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTPATHSOFFLINE
: Specifies the percentage of device class paths that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDISKSNOTRW
: Specifies the percentage of disks that are not writable for the disk device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDISKSUNAVAILABLE
: Specifies the percentage of the disk volumes that are unavailable, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

FILEDEVCLASSPCTSCRUNALLOCATABLE
: Specifies the percentage of scratch volumes that the server cannot allocate for a given non-shared file device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

Condition
: Specifies the condition that is used to compare the activity output to the specified value. The default value is EXISTS. Specify one of the following values:

EXists
: Creates a status monitoring indicator if the activity exists.

GT
: Creates a status monitoring indicator if the activity outcome is greater than the specified value.

GE
: Creates a status monitoring indicator if the activity outcome is greater than or equal to the specified value.

LT
: Creates a status monitoring indicator if the activity outcome is less than the specified value.

LE
: Creates a status monitoring indicator if the activity outcome is less than or equal to the specified value.

EQual
: Creates a status monitoring indicator if the activity outcome is equal to the specified value.

Value (Required)
: Specifies the value that is compared with the activity output for the specified condition. You must specify this parameter, unless CONDITION is set to EXISTS. You can specify an integer in the range 0 - 999999999999999.

STatus
: Specifies that the status indicator created in status monitoring if the condition that is being evaluated passes. This optional parameter has a default value of NORMAL. Specify one of the following values:

Normal
: Specifies that the status indicator has a normal status value.

Warning
: Specifies that the status indicator has a warning status value.

Error
: Specifies that the status indicator has an error status value.

Define status threshold

Define a status threshold for average storage pool utilization percentage by issuing the following command:

```
define statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=85
  condition=gt status=warning
```

Related commands

Table 1. Commands related to DEFINE STATUSTHRESHOLD

Command	Description

Command	Description
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

DEFINE STGPOOL (Define a storage pool)

Use this command to define a primary storage pool, copy storage pool, an active-data pool, a directory container storage pool, a container-copy storage pool, or a container storage pool in a cloud environment.

A primary storage pool provides a destination for backup files, archive files, or files that are migrated from client nodes. A copy storage pool provides a destination for copies of files that are in primary storage pools. An active-data pool provides a destination for active versions of backup data that are in primary storage pools. A container storage pool provides a destination for deduplicated files. A cloud storage pool provides storage in a cloud environment. A container-copy storage pool provides a tape copy of a directory-container storage pool. The maximum number of storage pools that you can define for a server is 999.

All volumes in a storage pool belong to the same device class. Random access storage pools use the DISK device type. After you define a random access storage pool, you must define volumes for the pool to create storage space.

Sequential access storage pools use device classes that you define for tape devices, files on disk (FILE device type), and storage on another server (SERVER device type). To create storage space in a sequential access storage pool, you must allow scratch volumes for the pool when you define or update it, or define volumes for the pool after you define the pool. You can also do both.

Restriction: If a client is using the simultaneous-write function and data deduplication, the data deduplication feature is disabled during backups to a storage pool.

The DEFINE STGPOOL command takes seven forms. The syntax and parameters for each form are defined separately.

Table 1. Commands related to DEFINE STGPOOL

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
COPY ACTIVEDATA	Copies active backup data.
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE DEVCLASS	Defines a device class.

Command	Description
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
DELETE STGPOOL	Deletes a storage pool from server storage.
MOVE DATA	Moves data from a specified storage pool volume to another storage pool volume.
MOVE MEDIA	Moves storage pool volumes that are managed by an automated library.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY DEVCLASS	Displays information about device classes.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY SHREDSTATUS	Displays information about data waiting to be shredded.
QUERY STGPOOL	Displays information about storage pools.
RENAME STGPOOL	Renames a storage pool.
REPAIR STGPOOL	Repairs a directory-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
SET DRMPRIMSTGPOOL	Specifies that primary storage pools are managed by DRM.
SHRED DATA	Manually starts the process of shredding deleted data.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

- DEFINE STGPOOL (Define a cloud-container storage pool)
  Use this command to define a container storage pool in a cloud environment. This type of storage pool is used for data deduplication. Cloud-container storage pools are not supported on Linux on System z®.
- DEFINE STGPOOL (Define a directory-container storage pool)
  Use this command to define a directory-container storage pool that is used for data deduplication.
- DEFINE STGPOOL (Define a container-copy storage pool)
  Use this command to define a container-copy storage pool to hold a copy of data from a directory-container storage pool.
- DEFINE STGPOOL (Define a primary storage pool assigned to random access devices)
  Use this command to define a primary storage pool that is assigned to random access devices.
- DEFINE STGPOOL (Define a primary storage pool assigned to sequential access devices)
  Use this command to define a primary storage pool that is assigned to sequential access devices.
- DEFINE STGPOOL (Define a copy storage pool assigned to sequential access devices)
  Use this command to define a copy storage pool that is assigned to sequential access devices.
- DEFINE STGPOOL (Define an active-data pool assigned to sequential-access devices)
  Use this command to define an active-data pool assigned to sequential-access devices.

DEFINE STGPOOL (Define a cloud-container storage pool)

Use this command to define a container storage pool in a cloud environment. This type of storage pool is used for data deduplication. Cloud-container storage pools are not supported on Linux on System z®.

Tip: To optimize backup and archive performance, set up one or more local storage directories to temporarily hold data that IBM Spectrum Protect™ is transferring to the cloud. After you use the DEFINE STGPOOL command to define a cloud-container storage pool, use the DEFINE STGPOOLDIRECTORY command to assign local storage directories to the cloud-container storage pool. For more information, see Optimizing performance for cloud object storage.

Privilege class

To issue this command, you must have system privilege.

Syntax

Notes:

1. If you specified CLOUDTYPE=AZURE, do not specify the IDENTITY parameter.
2. This parameter is valid only if you specify CLOUDTYPE=S3.
3. The default value of the ENCRYPT parameter is conditional. The server encrypts data by default if the CLOUDLOCATION parameter is set to OFFPREMISE. If the CLOUDLOCATION parameter is set to ONPREMISE, the default is No.

Parameters

pool_name (Required)
: Specifies the cloud-container storage pool to define. This parameter is required. The maximum length of the name is 30 characters.

STGType=CLoud (Required)
: Specifies the type of storage that you want to define for a cloud-container storage pool. To ensure that the storage pool can be used in a cloud environment, you must specify STGTYPE=CLOUD.
Tip: To optimize performance, set up one or more local storage directories to temporarily hold data that is moving to the cloud. After you define a cloud-container storage pool, use the DEFINE STGPOOLDIRECTORY command to assign local directories to the cloud-container storage pool.

POoltype=PRimary
: Specifies that you want to define a primary storage pool. This parameter is optional.

DESCription
: Specifies a description of the cloud-container storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains blank characters.

CLOUDType
: Specifies the type of cloud environment where you are configuring the storage pool.
You can specify one of the following values:

  AZure
  : Specifies that the storage pool uses a Microsoft Azure cloud computing system. If you define a storage pool as using Azure with this parameter, you cannot later change the storage pool type by using the UPDATE STGPOOL command.

  S3
  : Specifies that the storage pool uses a cloud computing system with the Simple Storage Service (S3) protocol, such as IBM® Cloud Object Storage or Amazon Web Services (AWS) S3. If you define a storage pool as using S3 with this parameter, you cannot later change the storage pool type by using the UPDATE STGPOOL command.

  IBMCLoudswift
  : Specifies that the storage pool uses an IBM Cloud cloud computing system with an OpenStack Swift cloud computing system.

  SWift
  : Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 2 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol that it is using.

  V1Swift
  : Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 1 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol that it is using.

  This parameter is optional. If you do not specify the parameter, the default value, SWIFT, is used.

CLOUDUrl
: Specifies the URL of the cloud environment where you are configuring the storage pool. Based on your cloud provider, you can use a blob service endpoint, region endpoint URL, an accesser IP address, a public authentication endpoint, or a similar value for this parameter. Be sure to include the protocol, such as `https://` or `http://`, at the beginning of the URL. The maximum length of the web address is 870 characters. The CLOUDURL parameter is not validated until the first backup begins.
For more information about how to locate these values, select your cloud service provider from the list on the Configuring a cloud-container storage pool for data storage page.
Tip: To use more than one IBM Cloud Object Storage accesser, list the accesser IP addresses separated by a vertical bar (|), with no spaces, such as in the following example:

  ```
  CLOUDURL=<accesser_URL1>|<accesser_URL2>|<accesser_URL3>
  ```

  If you are using the Operations Center, type an accesser IP address in the URL field of the Add Storage pool wizard, and then press Enter to add additional IP addresses. Use multiple accessers to improve performance.
  This parameter is required if you specify the CLOUDTYPE parameter.

  - AZure
  - S3 (Simple Storage Service)
  - IBMCLoudswift
  - SWift
  - V1Swift

IDentity
: Specifies the user ID for the cloud that is specified in the STGTYPE=CLOUD parameter. This parameter is required for all supported cloud computing systems except Azure. If you specified CLOUDTYPE=AZURE, do not specify the IDENTITY parameter. Based on your cloud provider, you can use an access key ID, a user name, a tenant name and user name, or a similar value for this parameter. The maximum length of the user ID is 255 characters.

PAssword (Required)
: Specifies the password for the cloud that is specified in the STGTYPE=CLOUD parameter. Based on your cloud provider, you can use a shared access signature (SAS) token, secret access key, an API key, a password, or a similar value for this parameter. This parameter is required. The maximum length of the password is 255 characters. The IDENTITY and PASSWORD parameters are not validated until the first backup begins.

CLOUDLocation
: Specifies the physical location of the cloud that is specified in the CLOUD parameter. This parameter is optional. The default value is OFFPREMISE. You can specify one of the following values:

  - OFfpremise
  - ONpremise

BUCKETName
: Specifies the name for an AWS S3 bucket or a IBM Cloud Object Storage vault to use with this storage pool, instead of using the default bucket name or vault name. This parameter is optional, and is valid only if you specify CLOUDTYPE=S3. If the name that you specify does not exist, the server creates a bucket or vault with the specified name before using the bucket or vault. Follow the naming restrictions for your cloud provider when specifying this parameter. Review the permissions for the bucket or vault and make sure that the credentials for this storage pool have permission to read, write, list, and delete objects in this bucket or vault. If you do not have the ability to change or view the permissions, and you have not already written data to this storage pool, use the UPDATE STGPOOL command with the BUCKETNAME parameter to use a different bucket or vault.

ACCess
: Specifies how client nodes and server processes access the cloud-container storage pool. This parameter is optional. The default value is READWRITE. You can specify one of the following values:

  READWrite
  : Specifies that client nodes and server processes can read and write to the cloud-container storage pool. This value is the default.

  READOnly
  : Specifies that client nodes and server processes can read only from the cloud-container storage pool.

  UNAVailable
  : Specifies that client nodes and server processes cannot access the cloud-container storage pool.

MAXWriters
: Specifies the maximum number of writing sessions that can run concurrently on the cloud-container storage pool. Specify a maximum number of writing sessions to control the performance of the cloud-container storage pool from negatively impacting other system resources. This parameter is optional. The default value is NOLIMIT. You can specify one of the following values:

  NOLimit
  : Specifies that no maximum size limit exists for the number of writers that you can use. This value is the default.

  maximum_writers
  : Limits the maximum number of writers that you can use. Specify an integer in the range 1 - 99999.

REUsedelay
: Specifies the number of days that must elapse after all deduplicated extents are removed from a cloud-container storage pool. This parameter controls the duration that deduplicated extents are associated with a cloud-container storage pool. When the value that is specified for the parameter expires, the deduplicated extents are deleted from the cloud-container storage pool. The default is 1. You can specify one of the following values:

  1
  : Specifies that deduplicated extents are deleted from a cloud-container storage pool after one day. This value is the default.

  days
  : You can specify an integer in the range 0 - 9999.

  Tip: Set this parameter to a value that is greater than the number specified for the SET DRMDBBACKUPEXPIREDAYS command. If you set this parameter to a higher value, you can ensure that when you restore the database to an earlier level, the references to files in the cloud-container storage pool are still valid.

ENCRypt
Specifies whether the server encrypts client data before it writes it to the storage pool. You can specify the following values:

Yes
Specifies that client data is encrypted by the server.
No
Specifies that client data is not encrypted by the server.

This parameter is optional. The default depends on the physical location of the cloud, which is specified by the CLOUDLOCATION parameter. If the cloud is off premise, the server encrypts data by default. If the cloud is on premises, the server does not encrypt data by default.

COMPRession
Specifies whether data is compressed in the storage pool. This parameter is optional. You can specify one of the following values:

No
Specifies that data is not compressed in the storage pool.
Yes
Specifies that data is compressed in the storage pool. This is the default.

Example 1: Define an OpenStack Swift cloud-container storage pool

Define an OpenStack Swift cloud-container storage pool that is named STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 description="OpenStack Swift cloud"
```

Example 2: Define a cloud-container primary storage pool

Define a cloud-container primary storage pool that is named STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 pooltype=primary
```

Example 3: Define a cloud-container storage pool with read only access

Define a cloud-container storage pool that is named STGPOOL1 with read only access.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 access=readonly
```

Example 4: Define a cloud-container storage pool with 99 writing sessions

Define a cloud-container storage pool that is named STGPOOL1 with 99 writing sessions.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 maxwr=99
```

Example 5: Define a cloud-container storage pool in which deduplicated extents are deleted after two days

Define a cloud-container storage pool that is named STGPOOL1 and deduplicated extents are deleted after two days.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 reusedelay=2
```

Related tasks:
Configuring a cloud-container storage pool for data storage
Related information:

AIX Linux Windows

DEFINE STGPOOL (Define a directory-container storage pool)

Use this command to define a directory-container storage pool that is used for data deduplication.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine STGpool--pool_name--STGType--=--DIrectory------------>

   .-POoltype--=--PRimary-.
>--+----------------------+--+---------------------------+---->
   '-POoltype--=--PRimary-'  '-DESCription--=--description-'

   .-ACCess--=--READWrite-------.
>--+-----------------------------+------------------------------>
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

   .-MAXSIze--=--NOLimit---------------.
>--+-----------------------------------+------------------------>
   '-MAXSIze--=--+-NOLimit-----------+-'
                 '-maximum_file_size-'

   .-MAXWriters--=--NOLimit-------------.
>--+-------------------------------------+---------------------->
   '-MAXWriters--=--+-NOLimit---------+-'
                    '-maximum_writers-'

>--+---------------------------+------------------------------->
   '-NEXTstgpool--=--pool_name-'

>--+-----------------------------------+------------------------>
   '-PROTECTstgpool--=--target_stgpool-'

>--+-------------------------------------------------+-------->
   |                          .-,--------------------. |
   |                          V                      | |
   '-PROTECTLOCalstgpools--=----local_target_stgpool-+-'

   .-REUsedelay--=--1----.  .-ENCRypt--=--No------.
>--+--------------------+--+---------------------+------------->
   '-REUsedelay--=--days-'  '-ENCRypt--=--+-Yes-+-'
                                          '-No--'

   .-COMPRession--=--Yes-----.
>--+-------------------------+-------------------------------><
   '-COMPRession--=--+-Yes-+-'
                     '-No--'
```

Parameters

pool_name (Required)
: Specifies the storage pool to define. This parameter is required. The maximum length of the name is 30 characters.

STGType=DIrectory (Required)
: Specifies the type of storage that you want to define for a storage pool. This parameter specifies that a directory-container type of storage pool is assigned to the storage pool. You must define a storage pool directory for this type of storage pool by using the DEFINE STGPOOLDIRECTORY command.
Requirements:

- Ensure that enough space is available on the file system for the directory-container storage pool.

- You must store the directory-container storage pool and the DB2® database on separate mount points on the file system. The directory-container storage pool might grow to occupy all the space on the directory it is stored on.
- You must use a file system other than the file system where the IBM Spectrum Protect™ server is located.

POoltype=PRimary
Specifies that you want the storage pool to be used as a primary storage pool. This parameter is optional.

DESCription
Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains blank characters.

ACCess
Specifies how client nodes and server processes can access the storage pool. This parameter is optional. You can specify one of the following values:

READWrite
Specifies that client nodes and server processes can read and write to the storage pool.

READOnly
Specifies that client nodes and server processes can read only from the storage pool.

UNAVailable
Specifies that client nodes and server processes cannot access the storage pool.

MAXSIze
Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. The default value is NOLIMIT. You can specify one of the following values:

NOLimit
Specifies that there is no maximum size limit for physical files that are stored in the storage pool.

maximum_file_size
Limits the maximum physical file size. Specify an integer in the range 1 - 999999, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 GB. You can use one of the following scale factors:

Table 1. Scale factor for the maximum file size

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

Tip: If you do not specify a unit of measurement for the maximum file size, the value is specified in bytes.

When the physical size of the storage pool exceeds the MAXSIZE parameter, the following table shows where files are typically stored.

Table 2. The location of a file according to the file size and the pool that is specified

Pool that is specified	Result
No pool is specified as the next storage pool in the hierarchy.	The server does not store the file.
A pool is specified as the next storage pool in the hierarchy.	The server stores the file in the storage pool that you specified.

Tip: If you also specify the NEXTstgpool parameter, define one storage pool in your hierarchy to have no limit on the maximum file size by specifying the MAXSIze=NOLimit parameter. When you have at least one pool with no size limit, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent during data deduplication processing, the server considers the size of the data deduplication process to be the file size. If the total size of all files in the process is larger than the maximum size limit, the server does not store the files in the storage pool.

MAXWriters
Specifies the maximum number of I/O threads for the following processes:

- The number of I/O threads that can run concurrently on the directory-container storage pool.
- The number of I/O threads that are written simultaneously to the directory-container storage pool.

This parameter is optional. As a best practice, use the default value of NOLIMIT. You can specify the following values:

NOLimit
: Specifies that no maximum number of I/O threads are written to the storage pool.

maximum_writers
: Limits the maximum number of I/O threads that you can use. Specify an integer in the range 1 - 99999.

Tip: The IBM Spectrum Protect server manages the number of I/O threads automatically based on the resources that are available and the server load.

NEXTstgpool
: Specifies the name of a random-access or primary sequential storage pool to which files are stored when the directory-container storage pool is full. This parameter is optional.
Restrictions:

- To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.
- If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
- Do not specify a directory-container or cloud-container storage pool.
- Do not use this parameter to specify a storage pool for data migration.

PROTECTstgpool
: Specifies the name of the directory-container storage pool on the target replication server where the data is backed up when you use the PROTECT STGPOOL command for this storage pool. This parameter is optional.

PROTECTLOCalstgpools
: Specifies the name of the container-copy storage pool on a local device where the data is backed up. This container-copy storage pool will be a local target storage pool when you use the PROTECT STGPOOL command. You can specify a maximum of two container-copy storage pool names. Separate multiple names with commas and no intervening spaces. The maximum length of each name is 30 characters. This parameter is optional.

REUsedelay
: Specifies the number of days that must elapse before all deduplicated extents are removed from a directory-container storage pool. This parameter controls the duration that deduplicated extents are associated with a directory-container storage pool after they are no longer referenced. When the value that is specified for the parameter expires, the deduplicated extents are deleted from the directory-container storage pool. Specify an integer in the range 0 - 9999. The default value for directory-container storage pools is 1, which means that deduplicated extents that are no longer referenced are deleted from a directory-container storage pool after 1 day.

  Set this parameter to a value greater than the number that is specified as your database backup period to ensure that data extents are still valid when you restore the database to another level.

ENCRypt
: Specifies whether the server encrypts client data before the server writes the data to the storage pool. You can specify the following values:

  Yes
  : Specifies that client data is encrypted by the server.

  No
  : Specifies that client data is not encrypted by the server. This is the default value.

COMPRession
: Specifies whether data is compressed in the storage pool. This parameter is optional. You can specify one of the following values:

  No
  : Specifies that data is not compressed in the storage pool.

  Yes
  : Specifies that data is compressed in the storage pool. This is the default.

Example: Define a directory-container storage pool that is configured for overflow storage when the storage pool is full

Define a directory-container storage pool that is named STGPOOL1. The storage pool is configured for overflow storage to a tape storage pool when the storage pool is full.

```
define stgpool stgpool1 stgtype=directory nextstgpool=overflow_tape_pool
```

Example: Define a directory-container storage pool that specifies the maximum file size

Define a directory-container storage pool that is named STGPOOL2. The storage pool specifies the maximum file size that the server can store in the storage pool as 100 megabytes.

```
define stgpool stgpool2 stgtype=directory maxsize=100M
```

Example: Define a directory-container storage pool on the source replication server with a directory-container storage pool on the target replication server to back up data

Define a directory-container storage pool that is named STGPOOL3. The data for storage pool STGPOOL3 is backed up to a directory-container storage pool, TARGET_STGPOOL3 on the target replication server.

```
define stgpool stgpool3 stgtype=directory protectstgpool=target_stgpool3
```

Example: Define a directory-container storage pool on the source replication server with a container-copy storage pool to back up data locally

Define a directory-container storage pool that is named STGPOOL3. The data for storage pool STGPOOL3 is backed up to a local container-copy storage pool, TARGET_LOCALSTGPOOL.

```
define stgpool stgpool3 stgtype=directory protectlocalstgpools=target_localstgpool
```

Example: Define a directory-container storage pool and disable compression

Define a directory-container storage pool that is named STGPOOL1 and disable compression.

```
define stgpool stgpool1 stgtype=directory compression=no
```

Table 3. Commands related to DEFINE STGPOOL (Define a directory-container storage pool)

Command	Description
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
QUERY CONTAINER	Displays information about a container.
QUERY STGPOOL	Displays information about storage pools.
REPAIR STGPOOL	Repairs a directory-container storage pool.
UPDATE STGPOOL (directory-container)	Update a directory-container storage pool.

DEFINE STGPOOL (Define a container-copy storage pool)

Use this command to define a container-copy storage pool to hold a copy of data from a directory-container storage pool.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine STGpool--pool_name--device_class_name----------------->

>--POoltype--=--COPYCONtainer--MAXSCRatch--=--number------------>
```

```
>--+-----------------------------+-----------------------------><
   '-DESCription--=--description-'

   .-ACCess--=--READWrite-------.
>--+-----------------------------+-----------------------------><
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

   .-PROTECTPRocess--=--2------.  .-RECLaim--=--100-----.
>--+-----------------------------+--+---------------------+------><
   '-PROTECTPRocess--=--number-'  '-RECLaim--=--percent-'

   .-RECLAIMLIMit--=--NOLimit-------.
>--+--------------------------------+---------------------------><
   '-RECLAIMLIMit--=--+-NOLimit---+-'
                      '-vol_limit-'

   .-REUsedelay--=--0----.
>--+---------------------+-------------------------------------><
   '-REUsedelay--=--days-'
```

Parameters

pool_name (Required)
: Specifies the name of the container-copy storage pool. The name must be unique, and the maximum length is 30 characters.

device_class_name (Required)
: Specifies the name of the sequential access device class to which this storage pool is assigned.
Restriction: You cannot specify the following device class types:

- DISK
- FILE
- CENTERA
- NAS
- REMOVABLEFILE
- SERVER

Restriction: Virtual tape libraries are not supported, regardless of which library type is defined. Only physical tape is supported.

POoltype=COPYCONtainer (Required)
: Specifies that you want to define a container-copy storage pool. A container-copy storage pool is used only to store a copy of data from a directory-container storage pool.

MAXSCRatch (Required)
: Specifies the maximum number of scratch volumes that the server can request for this storage pool. You can specify an integer in the range 0 - 100000000. If the server can request scratch volumes as needed, you do not have to define each volume to be used.

The value of this parameter is used to estimate the total number of volumes that are available in the storage pool and the corresponding estimated capacity for the storage pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. However, if the access mode for a scratch volume is OFFSITE, the volume is not deleted from the storage pool until the access mode is changed. An administrator can then query the server for empty, offsite scratch volumes and return them to the onsite location.

DESCription
: Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

ACCess
: Specifies how server processes such as storage-pool protection and repair can access data in the storage pool. This parameter is optional. The default value is READWRITE. You can specify one of the following values:

READWrite
: Specifies that the server can read and write to volumes in the storage pool.

READOnly

Specifies that the server can only read volumes in the storage pool. The server can use data in the storage pool to restore extents to directory-container storage pools. No operations that write to the container-copy storage pool are allowed.

UNAVailable
Specifies that the server cannot access data that is stored on volumes in the storage pool.

PROTECTPRocess
Specifies the maximum number of parallel processes that are used when you issue the PROTECT STGPOOL command to copy data to this pool from a directory-container storage pool. This parameter is optional. Enter a value in the range 1 - 20. The default value is 2.

The time that is required to complete the copy operation might be decreased by using multiple, parallel processes. However, in some cases when multiple processes are running, one or more of the processes must wait to use a volume that is already in use by a different process.

When you specify this value, consider the number of logical and physical drives that can be dedicated to the copy operation. To access a tape volume, the server uses a mount point and a drive. The number of available mount points and drives depends on the mount limit of the device class for the storage pool, and on other server and system activity.

This parameter is ignored if you use the PREVIEW=YES option on the PROTECT STGPOOL command. In that case, only one process is used and no mount points or drives are needed.

RECLaim
Specifies when a volume becomes eligible for reclamation and reuse. Specify eligibility as the percentage of a volume's space that is occupied by extents that are no longer stored in the associated directory-container storage pool. Reclamation moves any extents that are still stored in the associated directory-container storage pool from eligible volumes to other volumes. Reclamation occurs only when a PROTECT STGPOOL command stores data into this storage pool.

This parameter is optional. You can specify an integer in the range 1 - 100. The default value is 100, which means that volumes in this storage pool are not reclaimed.

The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

By setting the reclaim value to 50 percent or greater, data that is moved from two reclaimed volumes uses no more than the equivalent of one new volume.

Use caution when you use reclamation with container-copy storage pools that have offsite volumes. When an offsite volume becomes eligible for reclamation, in effect the server moves the extents on the volume back to the onsite location. If a disaster occurs onsite, the server can obtain extents from the offsite volume if the restored database refers to extents on the offsite volume. Therefore, for disaster recovery purposes, ensure that you schedule database backups to run after storage pool protection schedules and DRM move schedules have run, and ensure that all database backup volumes are taken offsite along with the DRM volumes.

Tip: Set different reclamation values for offsite container-copy storage pools and onsite container-copy storage pools. Because container-copy storage pools store deduplicated data, the data extents are spread across multiple tape volumes. When you choose a reclamation threshold for an offsite copy, carefully consider the number of available mount points and the number of tape volumes that you must retrieve if a disaster occurs. Setting a higher threshold means that you must retrieve more volumes than you would if your reclamation value was lower. Using a lower threshold reduces the number of mount points that are required in a disaster. The preferred method is to set the reclamation value for offsite copies to 60, and for onsite copies, in the range 90 - 100.

RECLAIMLIMit
Specifies the maximum number of volumes that the server reclaims when you issue the PROTECT STGPOOL command and specify the RECLAIM=YESLIMITED or RECLAIM=ONLYLIMITED option. This parameter is valid only for container-copy storage pools. This parameter is optional. The default value is NOLIMIT. You can specify one of the following values:

NOLimit
Specifies that all volumes in the container-copy storage pool are processed for reclamation.

vol_limit
Specifies the maximum number of volumes in the container-copy storage pool that are reclaimed. The value that you specify determines how many new scratch tapes are available after reclamation processing completes. You can specify a number in the range 1 - 100000.

REUsedelay

Specifies the number of days that must elapse after all extents are deleted from a volume before the volume can be rewritten or returned to scratch status. This parameter is optional. You can specify an integer in the range 0 - 9999. The default value is 0, which means that a volume can be rewritten or returned to scratch status as soon as all the extents are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to extents in the storage pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. If you use disaster recovery manager, the number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

Example: Define a container-copy storage pool with an LTO7A device class

Define a container-copy storage pool, CONTAINER1_COPY2, to the LTO7A device class. Allow up to 50 scratch volumes for this pool. Delay the reuse of volumes for 45 days.

```
define stgpool container1_copy2 lto7a pooltype=copycontainer
 maxscratch=50 reusedelay=45
```

Table 1. Commands related to DEFINE STGPOOL (Define a container-copy storage pool)

Command	Description
DEFINE STGPOOL (directory-container)	Define a directory-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
QUERY STGPOOL	Displays information about storage pools.
REPAIR STGPOOL	Repairs a directory-container storage pool.
UPDATE STGPOOL (container-copy)	Update a container-copy storage pool that stores copies of data from a directory-container storage pool.
UPDATE STGPOOL (directory-container)	Update a directory-container storage pool.

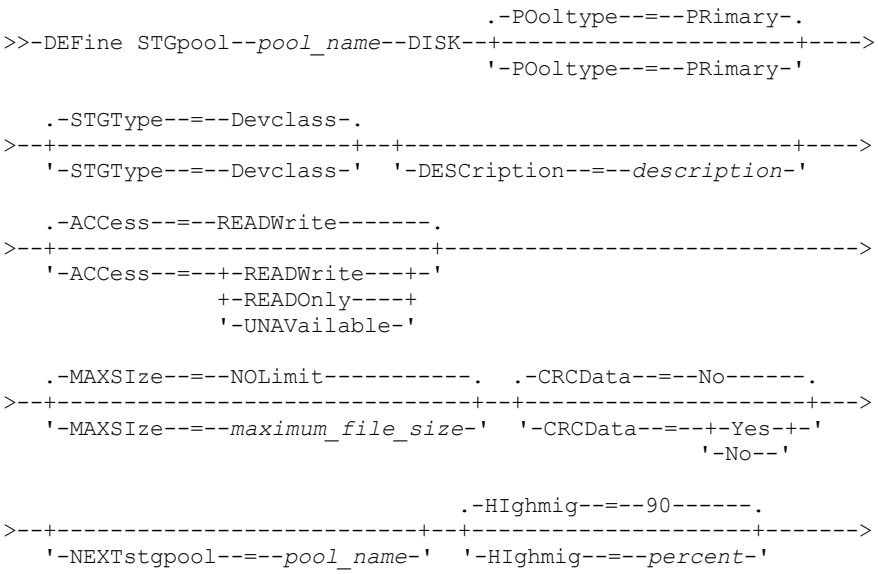
DEFINE STGPOOL (Define a primary storage pool assigned to random access devices)

Use this command to define a primary storage pool that is assigned to random access devices.

Privilege class

To issue this command, you must have system privilege.

Syntax



Notes:

1. This parameter is not available for CENTERA or SnapLock storage pools.
2. Linux This parameter is not available for SnapLock storage pools.

Parameters

pool_name (Required)
: Specifies the name of the storage pool to be defined. The name must be unique, and the maximum length is 30 characters.

DISK (Required)
: Specifies that you want to define a storage pool to the DISK device class (the DISK device class is predefined during installation).

POoltype=PRimary
: Specifies that you want to define a primary storage pool. This parameter is optional. The default value is PRIMARY.

STGType
: Specifies the type of storage that you want to define for a storage pool. This parameter is optional. The default value is DEVCLASS.

  Devclass
  : Specifies that a device class type of storage pool is assigned to the storage pool.

DESCription
: Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

ACCess
: Specifies how client nodes and server processes (such as migration and reclamation) can access files in the storage pool. This parameter is optional. The default value is READWRITE. You can specify the following values:

  READWrite

Specifies that client nodes and server processes can read and write to files stored on volumes in the storage pool.

READOnly
Specifies that client nodes can only read files from the volumes in the storage pool.

Server processes can move files within the volumes in the storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *readonly*, the storage pool is skipped when server processes attempt to write files to the storage pool.

UNAVailable
Specifies that client nodes cannot access files stored on volumes in the storage pool.

Server processes can move files within the volumes in the storage pool and can also move or copy files from this storage pool to another storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *unavailable*, the storage pool is skipped when server processes attempt to write files to the storage pool.

MAXSIze
Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. The default value is NOLIMIT. You can specify the following values:

NOLimit
Specifies that there is no maximum size limit for physical files that are stored in the storage pool.

maximum_file_size
Limits the maximum physical file size. Specify an integer 1 - 999999 terabytes, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 GB. You can use one of the following scale factors:

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

The client estimates the size of files that are sent to the server. The client estimate is used rather than the actual amount of data that is sent to the server. Client options, such as deduplication, compression, and encryption, can cause the actual amount of data that is sent to the server to be larger or smaller than the size estimate. For example, the compression of a file might be smaller in size than the estimate, thus sending less data than the estimate. Furthermore, a binary file might be larger in size after the compression processing, thus sending more data than the estimate.

When the physical size of the storage pool exceeds the MAXSIZE parameter, the following table shows where files are typically stored.

Table 1. The location of a file according to the file size and the pool that is specified

File size	Pool specified	Result
Exceeds the maximum size	No pool is specified as the next storage pool in the hierarchy	The server does not store the file
	A pool is specified as the next storage pool in the hierarchy	The server stores the file in the next storage pool that can accept the file size

Tip: If you also specify the NEXTstgpool parameter, define one storage pool in your hierarchy to have no limit on the maximum file size by specifying the MAXSIze=NOLimit parameter. When you have at least one pool with no size limit, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent in a single transaction, the server considers the size of the transaction to be the file size. If the total size of all files in the transaction is larger than the maximum size limit, the server does not store the files in the storage pool.

CRCData

Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

Yes
: Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more expenditure is required to calculate and compare CRC values between the storage pool and the server.

No
: Specifies that data is stored without CRC information.

NEXTstgpool
: Specifies a primary storage pool to which files are migrated. This parameter is optional.
If you do not specify a next storage pool, the following actions occur:

- The server cannot migrate files from this storage pool
- The server cannot store files that exceed the maximum size for this storage pool in another storage pool

Restrictions:

- To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.
- If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
- Do not specify a directory-container or cloud-container storage pool.
- Do not use this parameter to specify a storage pool for data migration.

HIghmig
: Specifies that the server starts migration for this storage pool when the amount of data in the pool reaches this percentage of the pool's estimated capacity. This parameter is optional. You can specify an integer 0 - 100. The default value is 90.

When the storage pool exceeds the high migration threshold, the server can start migration of files by node, to the next storage pool. The NEXTSTGPOOL parameter defines this setting. You can specify HIGHMIG=100 to prevent migration for this storage pool.

LOwmig
: Specifies that the server stops migration for this storage pool when the amount of data in the pool reaches this percentage of the pool's estimated capacity. This parameter is optional. You can specify an integer 0 - 99. The default value is 70.

When migration is by node or file space, depending upon collocation, the level of the storage pool can fall below the value that you specified for this parameter. To empty the storage pool, set LOWMIG=0.

CAChe
: Specifies whether the migration process leaves a cached copy of a file in this storage pool after you migrate the file to the next storage pool. This parameter is optional. The default value is NO. You can specify the following values:

Yes
: Specifies that caching is enabled.

No
: Specifies that caching is disabled.

Using cache might improve the ability to retrieve files, but might affect the performance of other processes.

MIGPRocess
: Specifies the number of processes that the server uses for migrating files from this storage pool. This parameter is optional. You can specify an integer 1 - 999. The default value is 1.

During migration, these processes are run in parallel to provide the potential for improved migration rates.

Tips:

- The number of migration processes is dependent upon the following settings:
  - The MIGPROCESS parameter
  - The collocation setting of the next pool
  - The number of nodes or the number of collocation groups with data in the storage pool that is being migrated

For example, suppose that `MIGPROCESS =6`, the next pool COLLOCATE parameter is set to NODE, but there are only two nodes with data on the storage pool. Migration processing consists of only two processes, not six. If the COLLOCATE parameter is set to GROUP and both nodes are in the same group, migration processing consists of only one process. If the COLLOCATE parameter is set to NO or FILESPACE, and each node has two file spaces with backup data, then migration processing consists of four processes.

- When you specify this parameter, consider whether the simultaneous-write function is enabled for server data migration. Each migration process requires a mount point and a drive for each copy storage pool and active-data pool that is defined to the target storage pool.

MIGDelay
: Specifies the minimum number of days a file must remain in a storage pool before it becomes eligible for migration. To calculate a value to compare to the specified MIGDELAY value, the server counts the following items:

  - The number of days that the file was in the storage pool
  - The number of days, if any, since the file was retrieved by a client

  The lesser of the two values are compared to the specified MIGDELAY value. For example, if all the following conditions are true, a file is not migrated:

  - A file was in a storage pool for five days.
  - The file was accessed by a client within the past three days.
  - The value that is specified for the MIGDELAY parameter is four days.

  This parameter is optional. You can specify an integer 0 - 9999. The default is 0, which means that you do not want to delay migration.

  If you want the server to count the number of days that are based on when a file was stored and not when it was retrieved, use the NORETRIEVEDATE server option.

MIGContinue
: Specifies whether you allow the server to migrate files that do not satisfy the migration delay time. This parameter is optional. The default is YES.

  Because you can require that files remain in the storage pool for a minimum number of days, the server may migrate all eligible files to the next storage pool yet not meet the low migration threshold. This parameter allows you to specify whether the server is allowed to continue the migration process by migrating files that do not satisfy the migration delay time.

  You can specify one of the following values:

  Yes
  : Specifies that, when necessary to meet the low migration threshold, the server continues to migrate files that do not satisfy the migration delay time.

    If you allow more than one migration process for the storage pool, some files that do not satisfy the migration delay time may be migrated unnecessarily. As one process migrates files that satisfy the migration delay time, a second process could begin migrating files that do not satisfy the migration delay time to meet the low migration threshold. The first process that is still migrating files that satisfy the migration delay time might have, by itself, caused the low migration threshold to be met.

  No
  : Specifies that the server stops migration when no eligible files remain to be migrated, even before reaching the low migration threshold. The server does not migrate files unless the files satisfy the migration delay time.

AUTOCopy
: Specifies when IBM Spectrum Protect™ runs simultaneous-write operations. The default value is CLIENT. This parameter is optional and affects the following operations:

  - Client store sessions
  - Server import processes
  - Server data-migration processes

  If an error occurs while data is being simultaneously written to a copy storage pool or active-data pool during a migration process, the server stops writing to the failing storage pools for the remainder of the process. However, the server continues to store files into the primary storage pool and any remaining copy storage pools or active-data pools. These

pools remain active for the duration of the migration process. Copy storage pools are specified using the COPYSTGPOOLS parameter. Active-data pools are specified using the ACTIVEDATAPOOLS parameter.

You can specify one of the following values:

None
: Specifies that the simultaneous-write function is disabled.

CLient
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions or server import processes. During server import processes, data is written simultaneously to only copy storage pools. Data is not written to active-data pools during server import processes.

MIGRation
: Specifies that data is written simultaneously to copy storage pools and active-data pools only during migration to this storage pool. During server data-migration processes, data is written simultaneously to copy storage pools and active-data pools only if the data does not exist in those pools. Nodes whose data is being migrated must be in a domain associated with an active-data pool. If the nodes are not in a domain associated with an active pool, the data cannot be written to the pool.

All
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions, server import processes, or server data-migration processes. Specifying this value ensures that data is written simultaneously whenever this pool is a target for any of the eligible operations.

COPYSTGpools
: Specifies the names of copy storage pools where the server simultaneously writes data. The COPYSTGPOOLS parameter is optional. You can specify a maximum of three copy pool names that are separated by commas. Spaces between the names of the copy pools are not allowed. When you specify a value for the COPYSTGPOOLS parameter, you can also specify a value for the COPYCONTINUE parameter.

  The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

  When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of copy storage pools and the COPYCONTINUE value from the primary storage pool. The primary storage pool is specified by the copy group of the management class that is bound to the data.

  The server can write data simultaneously to copy storage pools during the following operations:

  - Back up and archive operations by IBM Spectrum Protect backup-archive clients or application clients that are using the IBM Spectrum Protect API
  - Migration operations by IBM Spectrum Protect for Space Management clients
  - Import operations that involve copying exported file data from external media to a primary storage pool associated with a copy storage pool list

  Restriction: The simultaneous-write function is not supported for the following store operations:

  - When the operation is using LAN-free data movement. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is followed.
  - NAS backup operations. If the primary storage pool specified in the DESTINATION or TOCDESTINATION in the copy group of the management class has copy storage pools that are defined:
    - The copy storage pools are ignored
    - The data is stored into the primary storage pool only

  Attention: The function that is provided by the COPYSTGPOOLS parameter is not intended to replace the BACKUP STGPOOL command. If you use the COPYSTGPOOLS parameter, continue to use the BACKUP STGPOOL command to ensure that the copy storage pools are complete copies of the primary storage pool. There are cases when a copy might not be created. For more information, see the COPYCONTINUE parameter description.

COPYContinue
: Specifies how the server usually reacts to a copy storage pool write failure for any of the copy storage pools that are listed in the COPYSTGPOOLS parameter. This parameter is optional. The default value is YES. When you specify the COPYCONTINUE parameter, you must also specify the COPYSTGPOOLS parameter.
  You can specify the following values:

  Yes

If the COPYCONTINUE parameter is set to YES, the server will stop writing to the failing copy pools for the remainder of the session, but continue storing files into the primary pool and any remaining copy pools. The copy storage pool list is active only for the life of the client session and applies to all the primary storage pools in a particular storage pool hierarchy.

No

If the COPYCONTINUE parameter is set to NO, the server will fail the current transaction and discontinue the store operation.

Restrictions:

- The setting of the COPYCONTINUE parameter does not affect active-data pools. If a write failure occurs for any of the active-data pools, the server stops writing to the failing active-data pool for the remainder of the session, but continues storing files into the primary pool and any remaining active-data pools and copy storage pools. The active-data pool list is active only for the life of the session and applies to all the primary storage pools in a particular storage pool hierarchy.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server import. If data is being written simultaneously and a write failure occurs to the primary storage pool or any copy storage pool, the server import process fails.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server data migration. If data is being written simultaneously and a write failure occurs to any copy storage pool or active-data pool, the failing storage pool is removed and the data migration process continues. Write failures to the primary storage pool cause the migration process to fail.

ACTIVEDATApools

Specifies the names of active-data pools where the server simultaneously writes data during a client backup operation. The ACTIVEDATAPOOLS parameter is optional. Spaces between the names of the active-data pools are not allowed.

The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of active-data pools from the destination storage pool that is specified in the copy group. The primary storage pool is specified by the copy group of the management class that is bound to the data.

The server can write data simultaneously to active-data pools only during backup operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API.
Restrictions:

1. This parameter is available only to primary storage pools that use "NATIVE" or "NONBLOCK" data format. This parameter is not available for storage pools that use the following data formats:
   - NETAPPDUMP
   - CELERRADUMP
   - NDMPDUMP
2. Writing data simultaneously to active-data pools is not supported when you use LAN-free data movement. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is followed.
3. The simultaneous-write function is not supported when a NAS backup operation is writing a TOC file. If the primary storage pool specified in the TOCDESTINATION in the copy group of the management class has active-data pools that are defined:
   - The active-data pools are ignored
   - The data is stored into the primary storage pool only
4. You cannot use the simultaneous-write function with CENTERA storage devices.
5. Data that is being imported is not stored in active-data pools. After an import operation, use the COPY ACTIVEDATA command to store the imported data in an active-data pool.

Attention: The function that is provided by the ACTIVEDATAPOOLS parameter is not intended to replace the COPY ACTIVEDATA command. If you use the ACTIVEDATAPOOLS parameter, use the COPY ACTIVEDATA command to ensure that the active-data pools contain all active data of the primary storage pool.

SHRED

Specifies whether data is physically overwritten when it is deleted. This parameter is optional. You can specify an integer 0 - 10. The default value is 0.

If you specify a value of zero, the server deletes the data from the database. However, the storage that is used to contain the data is not overwritten, and the data exists in storage until that storage is reused for other data. It might be possible to

discover and reconstruct the data after it is deleted.

If you specify a value greater than zero, the server deletes the data both logically and physically. The server overwrites the storage that is used to contain the data the specified number of times. This overwriting increases the difficulty of discovering and reconstructing the data after it is deleted.

To ensure that all copies of the data are shredded, specify a SHRED value greater than zero for the storage pool that is specified in the NEXTSTGPOOL parameter. Do not specify either the COPYSTGPOOLS or ACTIVEDATAPOOLS. Specifying relatively high values for the overwrite count generally improves the level of security, but might affect performance adversely.

Overwriting of deleted data is done asynchronously after the delete operation is complete. Therefore, the space that is occupied by the deleted data remains occupied for some time. The space is not available as free space for new data.

A SHRED value greater than zero cannot be used if the value of the CACHE parameter is YES.

Important: After an export operation finishes and identifies files for export, any change to the storage pool SHRED value is ignored. An export operation that is suspended retains the original SHRED value throughout the operation. You might want to consider canceling your export operation if changes to the storage pool SHRED value jeopardize the operation. You can reissue the export command after any needed cleanup.

Example: Define a primary storage pool for a DISK device class

Define a primary storage pool, POOL1, to use the DISK device class, with caching enabled. Limit the maximum file size to 5 MB. Store any files larger than 5 MB in subordinate storage pools that begin with the PROG2 storage pool. Set the high migration threshold to 70 percent, and the low migration threshold to 30 percent.

```
define stgpool pool1 disk
 description="main disk storage pool" maxsize=5m
 highmig=70 lowmig=30 cache=yes
 nextstgpool=prog2
```

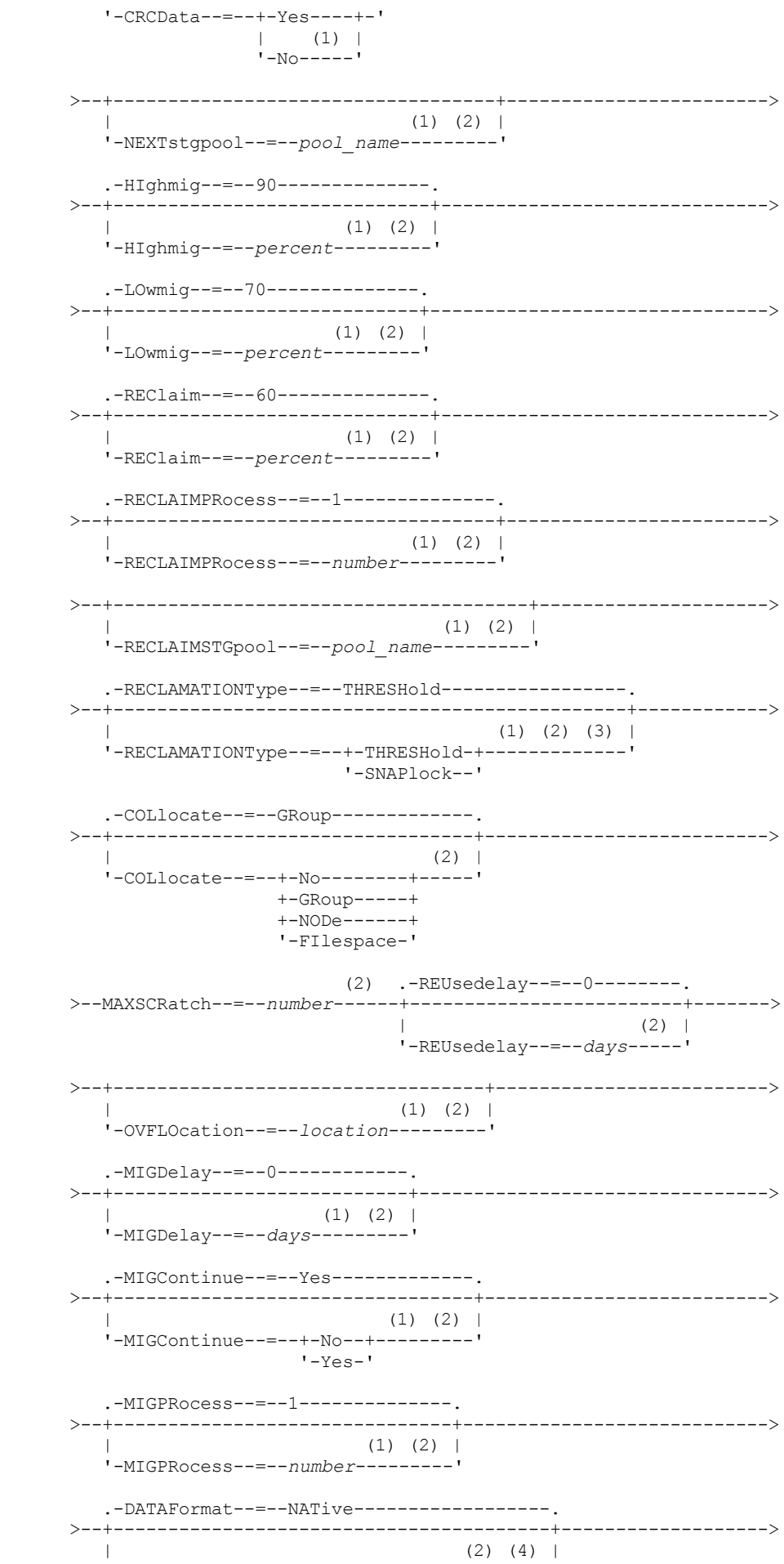
DEFINE STGPOOL (Define a primary storage pool assigned to sequential access devices)

Use this command to define a primary storage pool that is assigned to sequential access devices.

Privilege class

To issue this command, you must have system privilege.

Syntax


'-CRCData--=--+-Yes----+-'
(1)
'-No-----'
>--+----------+-->
(1) (2)
'-NEXTstgpool--=--pool_name---------'
.-HIghmig--=--90--------------.
>--+----------+-->
(1) (2)
'-HIghmig--=--percent---------'
.-LOwmig--=--70--------------.
>--+----------+-->
(1) (2)
'-LOwmig--=--percent---------'
.-RECLaim--=--60--------------.
>--+----------+-->
(1) (2)
'-RECLaim--=--percent---------'
.-RECLAIMPRocess--=--1--------------.
>--+----------+-->
(1) (2)
'-RECLAIMPRocess--=--number---------'
>--+----------+-->
(1) (2)
'-RECLAIMSTGpool--=--pool_name---------'
.-RECLAMATIONType--=--THRESHold-----------------.
>--+----------+-->
(1) (2) (3)
'-RECLAMATIONType--=--+-THRESHold-+-------------'
'-SNAPlock--'
.-COLlocate--=--GRoup-------------.
>--+----------+-->
(2)
'-COLlocate--=--+-No--------+-----'
+-GRoup-----+
+-NODe------+
'-FIlespace-'
(2) .-REUsedelay--=--0--------.
>--MAXSCRatch--=--number------+----------+-------->
(2)
'-REUsedelay--=--days-----'
>--+----------+-->
(1) (2)
'-OVFLOcation--=--location---------'
.-MIGDelay--=--0-------------.
>--+----------+-->
(1) (2)
'-MIGDelay--=--days---------'
.-MIGContinue--=--Yes-------------.
>--+----------+-->
(1) (2)
'-MIGContinue--=--+-No--+---------'
'-Yes-'
.-MIGPRocess--=--1--------------.
>--+----------+-->
(1) (2)
'-MIGPRocess--=--number---------'
.-DATAFormat--=--NATive------------------.
>--+----------+-->
(2) (4)

Notes:

1. This parameter is not available for storage pools that use the data formats NETAPPDUMP, CELERRADUMP, or NDMPDUMP.
2. This parameter is not available or is ignored for CENTERA storage pools.
3. The RECLAMATIONTYPE=SNAPLOCK setting is valid only for storage pools that are defined to servers that are enabled for IBM Spectrum Protect™ for Data Retention. The storage pool must be assigned to a FILE device class, and the directories that are specified in the device class must be NetApp SnapLock volumes.
4. The values NETAPPDUMP, CELERRADUMP, and NDMPDUMP are not valid for storage pools that are defined with a FILE-type device class.
5. This parameter is valid only for storage pools that are defined with a FILE-type device class.
6. This parameter is available only when the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
: Specifies the name of the storage pool to be defined. The name must be unique, and the maximum length is 30 characters.

device_class_name (Required)
: Specifies the name of the device class to which this storage pool is assigned. You can specify any device class except for the DISK device class.

POoltype=PRimary
: Specifies that you want to define a primary storage pool. This parameter is optional. The default value is PRIMARY.

STGType
: Specifies the type of storage that you want to define for a storage pool. This parameter is optional. The default value is DEVCLASS.

  Devclass
  : Specifies that a device class type of storage pool is assigned to the storage pool.

DESCription
Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

ACCess
Specifies how client nodes and server processes (such as migration and reclamation) can access files in the storage pool. This parameter is optional. The default value is READWRITE. You can specify the following values:

READWrite
Specifies that client nodes and server processes can read and write to files stored on volumes in the storage pool.

READOnly
Specifies that client nodes can only read files from the volumes in the storage pool.

Server processes can move files within the volumes in the storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *readonly*, the storage pool is skipped when server processes attempt to write files to the storage pool.

UNAVailable
Specifies that client nodes cannot access files stored on volumes in the storage pool.

Server processes can move files within the volumes in the storage pool and can also move or copy files from this storage pool to another storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *unavailable*, the storage pool is skipped when server processes attempt to write files to the storage pool.

MAXSIze
Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. The default value is NOLIMIT. You can specify one of the following values:

NOLimit
Specifies that there is no maximum size limit for physical files stored in the storage pool.

maximum_file_size
Limits the maximum physical file size. Specify an integer from 1 to 999999 terabytes, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 gigabytes. Scale factors are:

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

The client estimates the size of files that are sent to the server. The client estimate is used rather than the actual amount of data that is sent to the server. Client options, such as deduplication, compression, and encryption, can cause the actual amount of data that is sent to the server to be larger or smaller than the size estimate. For example, the compression of a file might be smaller in size than the estimate, thus sending less data than the estimate. Furthermore, a binary file might be larger in size after the compression processing, thus sending more data than the estimate.

When the physical size of the storage pool exceeds the MAXSIZE parameter, the following table shows where files are typically stored.

Table 1. The location of a file according to the file size and the pool that is specified

File size	Pool specified	Result
Exceeds the maximum size	No pool is specified as the next storage pool in the hierarchy	The server does not store the file
	A pool is specified as the next storage pool in the hierarchy	The server stores the file in the next storage pool that can accept the file size

Tip: If you also specify the NEXTstgpool parameter, define one storage pool in your hierarchy to have no limit on the maximum file size by specifying the MAXSIze=NOLimit parameter. When you have at least one pool with no size limit, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent in a single transaction, the server considers the size of the transaction to be the file size. If the total size of all files in the transaction is larger than the maximum size limit, the server does not store the files in the storage pool.

Restriction:

This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCData
: Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

  Yes
  : Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

  No
  : Specifies that data is stored without CRC information.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

  Tip:

  For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

  To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

  - IBM® LTO5 and later.
  - IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
  - Oracle StorageTek T10000C and T10000D drives.

NEXTstgpool
: Specifies a primary storage pool to which files are migrated. You cannot migrate data from a sequential access storage pool to a random access storage pool. This parameter is optional.

  If this storage pool does not have a next storage pool, the server cannot migrate files from this storage pool and cannot store files that exceed the maximum size for this storage pool in another storage pool.

  When there is insufficient space available in the current storage pool, the NEXTSTGPOOL parameter for sequential access storage pools does not allow data to be stored into the next pool. In this case, the server issues a message and the transaction fails.

  For next storage pools with a device type of FILE, the server completes a preliminary check to determine whether sufficient space is available. If space is not available, the server skips to the next storage pool in the hierarchy. If space is available, the server attempts to store data in that pool. However, it is possible that the storage operation might fail because, at the time the actual storage operation is attempted, the space is no longer available.

  Restrictions:

  - To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.

- If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
- Do not specify a directory-container or cloud-container storage pool.
- Do not use this parameter to specify a storage pool for data migration.
- This parameter is not available for storage pools that use the following data formats:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

HIghmig
: Specifies that the server starts migration when storage pool utilization reaches this percentage. For sequential-access disk (FILE) storage pools, utilization is the ratio of data in a storage pool to the pool's total estimated data capacity, including the capacity of all scratch volumes specified for the pool. For storage pools that use tape media, utilization is the ratio of volumes that contain data to the total number of volumes in the storage pool. The total number of volumes includes the maximum number of scratch volumes. This parameter is optional. You can specify an integer 0 - 100. The default value is 90.

  When the storage pool exceeds the high migration threshold, the server can start migration of files by volume to the next storage pool defined for the pool. You can set the high migration threshold to 100 to prevent migration for the storage pool.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

LOwmig
: Specifies that the server stops migration when storage pool utilization is at or below this percentage. For sequential-access disk (FILE) storage pools, utilization is the ratio of data in a storage pool to the pool's total estimated data capacity, including the capacity of all scratch volumes specified for the pool. For storage pools that use tape media, utilization is the ratio of volumes that contain data to the total number of volumes in the storage pool. The total number of volumes includes the maximum number of scratch volumes. This parameter is optional. You can specify an integer 0 - 99. The default value is 70.

  When the storage pool reaches the low migration threshold, the server does not start migration of files from another volume. You can set the low migration threshold to 0 to allow migration to empty the storage pool.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

RECLaim
: Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the database.

  Reclamation makes the fragmented space on volumes usable again by moving any remaining unexpired files from one volume to another volume, thus making the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100. The default value is 60, except for storage pools that use WORM devices.

  AIX Windows For storage pools that use a WORM device class, you can lower the value from the default of 100. Lowering the value allows the server to consolidate data onto fewer volumes when needed. Volumes that are emptied by reclamation can be checked out of the library, freeing slots for new volumes. Because the volumes are write-once, the volumes cannot be reused.

  The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

  Specify a value of 50 percent or greater for this parameter so that files stored on two volumes can be combined onto a single output volume.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP

- NDMPDUMP

RECLAIMPRocess
: Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999. The default value is 1. You can specify one or more reclamation processes for each primary sequential-access storage pool.
When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

  - The number of sequential storage pools.
  - The number of logical and physical drives that can be dedicated to the operation.

  To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

  For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Assuming that the RECLAIMSTGPOOL parameter is not specified or that the reclaim storage pool has the same device class as the storage pool that is being reclaimed, each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for the storage pools must have a mount limit of at least 16.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

RECLAIMSTGpool
: Specifies another primary storage pool as a target for reclaimed data from this storage pool. This parameter is optional. When the server reclaims volumes for the storage pool, the server moves unexpired data from the volumes that are being reclaimed to the storage pool named with this parameter.

  A reclaim storage pool is most useful for a storage pool that has only one drive in its library. When you specify this parameter, the server moves all data from reclaimed volumes to the reclaim storage pool regardless of the number of drives in the library.

  To move data from the reclaim storage pool back to the original storage pool, use the storage pool hierarchy. Specify the original storage pool as the next storage pool for the reclaim storage pool.

  Restriction:

  - This parameter is not available for storage pools that use the following data formats:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

RECLAMATIONType
: Specifies the method by which volumes are reclaimed and managed. This parameter is optional. The default value is THRESHOLD. The following are possible values:

  THRESHold
  : Specifies that volumes that belong to this storage pool are reclaimed based on the threshold value in the RECLAIM attribute for this storage pool.

  SNAPlock
  : Specifies that FILE volumes that belong to this storage pool are managed for retention using NetApp Data ONTAP software and NetApp SnapLock volumes. This parameter is only valid for storage pools that are defined to a server that has data retention protection enabled and that is assigned to a FILE device class. Volumes in this storage pool are not reclaimed based on threshold; the RECLAIM value for the storage pool is ignored.

    All volumes in this storage pool are created as FILE volumes. A retention date, which is derived from the retention attributes in the archive copy group for the storage pool, is set in the metadata for the FILE volume by using the SnapLock feature of the NetApp Data ONTAP operating system. Until the retention date expires, the FILE volume and any data on it cannot be deleted from the physical SnapLock volume on which it is stored.

The RECLAMATIONTYPE parameter for all storage pools that are being defined must be the same when defined to the same device class name. The DEFINE command can fail if the RECLAMATIONTYPE parameter specified is different from what is defined for storage pools that are already defined to the device class name.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate

Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

- A single client node
- A group of file spaces
- A group of client nodes
- A client file space

This parameter is optional. The default value is GROUP.

Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required. Collocation can also impact the number of processes migrating disks to sequential pool.

You can specify one of the following options:

No

Specifies that collocation is disabled. During migration from disk, processes are created at a file space level.

GRoup

Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
- Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.
- During migration from disk, the server creates migration processes at the collocation group level for grouped nodes, and at the node level for ungrouped nodes.

If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
- Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces that are named A, B, C, D, and E. File spaces A and B belong to a file space collocation group but C, D, and E do not. File spaces A and B are collocated by file space collocation group, while C, D, and E are collocated by node.
- During migration from disk, the server creates migration processes at the collocation group level for grouped file spaces.

Data is collocated on the least number of sequential access volumes.

NODe

Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

For COLLOCATE=NODE, the server creates processes at the node level when you migrate data from disk.

FIlespace
Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

For COLLOCATE=FILESPACE, the server creates processes at the file space level when you migrate data from disk.

MAXSCRatch (Required)
Specifies the maximum number of scratch volumes that the server can request for this storage pool. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes, you avoid having to define each volume to be used.

The value that is specified for this parameter is used to estimate the total number of volumes available in the storage pool and the corresponding estimated capacity for the storage pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. When scratch volumes with the device type of FILE are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay
Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. The default value is 0, which means that a volume can be rewritten or returned to the scratch pool as soon as all the files are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to files in the storage pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. The number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

OVFLOcation
Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.
Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGDelay
Specifies the minimum number of days a file must remain in a storage pool before it becomes eligible for migration. All files on a volume must be eligible for migration before the server selects the volume for migration. To calculate a value to compare to the specified MIGDELAY, the server counts the number of days that the file has been in the storage pool.

This parameter is optional. You can specify an integer 0 - 9999. The default is 0, which means that you do not want to delay migration. If you want the server to count the number of days that are based only on when a file was stored and not when it was retrieved, use the NORETRIEVEDATE server option.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue
: Specifies whether you allow the server to migrate files that do not satisfy the migration delay time. This parameter is optional. The default is YES.

  Because you can require that files remain in the storage pool for a minimum number of days, the server may migrate all eligible files to the next storage pool yet not meet the low migration threshold. This parameter allows you to specify whether the server is allowed to continue the migration process by migrating files that do not satisfy the migration delay time.

  You can specify one of the following values:

  Yes
  : Specifies that, when necessary to meet the low migration threshold, the server continues to migrate files that do not satisfy the migration delay time.

    If you allow more than one migration process for the storage pool, some files that do not satisfy the migration delay time may be migrated unnecessarily. As one process migrates files that satisfy the migration delay time, a second process could begin migrating files that do not satisfy the migration delay time to meet the low migration threshold. The first process that is still migrating files that satisfy the migration delay time might have, by itself, caused the low migration threshold to be met.

  No
  : Specifies that the server stops migration when no eligible files remain to be migrated, even before reaching the low migration threshold. The server does not migrate files unless the files satisfy the migration delay time.

MIGPRocess
: Specifies the number of parallel processes to use for migrating the files from the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999. The default value is 1.

  When calculating the value for this parameter, consider the number of sequential storage pools that will be involved with the migration, and the number of logical and physical drives that can be dedicated to the operation. To access a sequential-access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect and system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the migration.

  For example, suppose you want to simultaneously migrate the files from volumes in two primary sequential storage pools and that you want to specify three processes for each of the storage pools. The storage pools have the same device class. Assuming that the storage pool to which files are being migrated has the same device class as the storage pool from which files are being migrated, each process requires two mount points and, if the device type is not FILE, two drives. (One drive is for the input volume, and the other drive is for the output volume.) To run six migration processes simultaneously, you need a total of at least 12 mount points and 12 drives. The device class for the storage pools must have a mount limit of at least 12.

  If the number of migration processes you specify is more than the number of available mount points or drives, the processes that do not obtain mount points or drives will wait for mount points or drives to become available. If mount points or drives do not become available within the MOUNTWAIT time, the migration processes will end. For information about specifying the MOUNTWAIT time, see DEFINE DEVCLASS (Define a device class).

  The IBM Spectrum Protect server will start the specified number of migration processes regardless of the number of volumes that are eligible for migration. For example, if you specify ten migration processes and only six volumes are eligible for migration, the server will start ten processes and four of them will complete without processing a volume.

  Tip: When you specify this parameter, consider whether the simultaneous-write function is enabled for server data migration. Each migration process requires a mount point and a drive for each copy storage pool and active-data pool that is defined to the target storage pool.
  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

DATAFormat
Specifies the data format to use to back up files to this storage pool and restore files from this storage pool. The default format is the NATIVE server format. You can specify the following values:

NATive
Specifies the data format is the native IBM Spectrum Protect server format and includes block headers.
NONblock
Specifies the data format is the native IBM Spectrum Protect server format and does not include block headers. The default minimum block size on a volume that is associated with a FILE device class is 256 KB, regardless how much data is written to the volume. For certain tasks, you can minimize wasted space on storage volumes by specifying the NONBLOCK data format. For example, you can specify the NONBLOCK data format for the following tasks:

- Using content-management products
- Using the DIRMC client option to store directory information
- Migrating very small files by using IBM Spectrum Protect for Space Management or IBM Spectrum Protect HSM for Windows

In most situations, however, the NATIVE format is preferred.
NETAPPDump
Specifies the data is in a NetApp dump format. This data format must be specified for file system images that are in a dump format and that were backed up from a NetApp or an IBM System Storage® N Series file server that uses NDMP. The server does not complete migration, reclamation, or AUDIT VOLUME for a storage pool with DATAFORMAT=NETAPPDUMP. You can use the MOVE DATA command to move data from one primary storage pool to another, or out of a volume if the volume must be reused.
CELERRADump
Specifies that the data is in an EMC Celerra dump format. This data format must be specified for file system images that are in a dump format and that were backed up from an EMC Celerra file server that uses NDMP. The server does not complete migration, reclamation, or AUDIT VOLUME for a storage pool with DATAFORMAT=CELERRADUMP. You can use the MOVE DATA command to move data from one primary storage pool to another, or out of a volume if the volume must be reused.
NDMPDump
Specifies that the data is in NAS vendor-specific backup format. Use this data format for file system images that were backed up from a NAS file server other than a NetApp or EMC Celerra file server. The server does not complete migration, reclamation, or AUDIT VOLUME for a storage pool with DATAFORMAT=NDMPDUMP. You can use the MOVE DATA command to move data from one primary storage pool to another, or out of a volume if the volume must be reused.

AUTOCopy
Specifies when IBM Spectrum Protect completes simultaneous-write operations. The default value is CLIENT. This parameter is optional and affects the following operations:

- Client store sessions
- Server import processes
- Server data-migration processes

If the AUTOCOPY option is set to `ALL` or `CLIENT`, and there is at least one storage pool that is listed in the COPYSTGPOOLS or ACTIVEDATAPOOLS options, any client-side deduplication is disabled.

If an error occurs while data is being simultaneously written to a copy storage pool or active-data pool during a migration process, the server stops writing to the failing storage pools for the remainder of the process. However, the server continues to store files into the primary storage pool and any remaining copy storage pools or active-data pools. These pools remain active for the duration of the migration process. Copy storage pools are specified using the COPYSTGPOOLS parameter. Active-data pools are specified using the ACTIVEDATAPOOLS parameter.

You can specify one of the following values:

None
Specifies that the simultaneous-write function is disabled.
CLient
Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions or server import processes. During server import processes, data is written simultaneously to only copy storage pools. Data is not written to active-data pools during server import processes.
MIGRation

Specifies that data is written simultaneously to copy storage pools and active-data pools only during migration to this storage pool. During server data-migration processes, data is written simultaneously to copy storage pools and active-data pools only if the data does not exist in those pools. Nodes whose data is being migrated must be in a domain associated with an active-data pool. If the nodes are not in a domain associated with an active pool, the data cannot be written to the pool.

All

Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions, server import processes, or server data-migration processes. Specifying this value ensures that data is written simultaneously whenever this pool is a target for any of the eligible operations.

COPYSTGpools

Specifies the names of copy storage pools where the server simultaneously writes data. The COPYSTGPOOLS parameter is optional. You can specify a maximum of three copy pool names that are separated by commas. Spaces between the names of the copy pools are not allowed. When you specify a value for the COPYSTGPOOLS parameter, you can also specify a value for the COPYCONTINUE parameter.

The combined total number of storage pools that are specified in the COPYSTGPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of copy storage pools and the COPYCONTINUE value from the primary storage pool. The primary storage pool is specified by the copy group of the management class that is bound to the data.

The server can write data simultaneously to copy storage pools during the following operations:

- Back up and archive operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API
- Migration operations by IBM Spectrum Protect for Space Management clients
- Import operations that involve copying exported file data from external media to a storage pool defined with a copy storage pool list

Restrictions:

1. This parameter is available only to primary storage pools that use NATIVE or NONBLOCK data format. This parameter is not available for storage pools that use the following data formats:
   - NETAPPDUMP
   - CELERRADUMP
   - NDMPDUMP
2. Writing data simultaneously to copy storage pools is not supported when LAN-free data movement is used. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is accepted.
3. The simultaneous-write function is not supported for NAS backup operations. If the primary storage pool specified in the DESTINATION or TOCDESTINATION in the copy group of the management class has copy storage pools defined, the copy storage pools are ignored and the data is stored into the primary storage pool only.
4. You cannot use the simultaneous-write function with CENTERA storage devices.

Attention: The function that is provided by the COPYSTGPOOLS parameter is not intended to replace the BACKUP STGPOOL command. If you use the COPYSTGPOOLS parameter, continue to use the BACKUP STGPOOL command to ensure that the copy storage pools are complete copies of the primary storage pool. There are cases when a copy might not be created. For more information, see the COPYCONTINUE parameter description.

COPYContinue

Specifies how the server reacts to a copy storage pool write failure for any of the copy storage pools that are listed in the COPYSTGPOOLS parameter. This parameter is optional. The default value is YES. When you specify the COPYCONTINUE parameter, you must also specify the COPYSTGPOOLS parameter.

The COPYCONTINUE parameter has no effect on the simultaneous-write function during migration.

You can specify the following values:

Yes

If the COPYCONTINUE parameter is set to YES, the server will stop writing to the failing copy pools for the remainder of the session, but continue storing files into the primary pool and any remaining copy pools. The copy storage pool list is active only for the life of the client session and applies to all the primary storage pools in a particular storage pool hierarchy.

No

If the COPYCONTINUE parameter is set to NO, the server will fail the current transaction and discontinue the store operation.

Restrictions:

- The setting of the COPYCONTINUE parameter does not affect active-data pools. If a write failure occurs for any of the active-data pools, the server stops writing to the failing active-data pool for the remainder of the session, but continues storing files into the primary pool and any remaining active-data pools and copy storage pools. The active-data pool list is active only for the life of the session and applies to all the primary storage pools in a particular storage pool hierarchy.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server import. If data is being written simultaneously and a write failure occurs to the primary storage pool or any copy storage pool, the server import process fails.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server data migration. If data is being written simultaneously and a write failure occurs to any copy storage pool or active-data pool, the failing storage pool is removed and the data migration process continues. Write failures to the primary storage pool cause the migration process to fail.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

ACTIVEDATApools
: Specifies the names of active-data pools where the server simultaneously writes data during a client backup operation. The ACTIVEDATAPOOLS parameter is optional. Spaces between the names of the active-data pools are not allowed.

  The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

  When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of active-data pools from the destination storage pool specified in the copy group. The primary storage pool is specified by the copy group of the management class that is bound to the data.

  The server can write data simultaneously to active-data pools only during backup operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API.
  Restrictions:

  1. This parameter is available only to primary storage pools that use NATIVE or NONBLOCK data format. This parameter is not available for storage pools that use the following data formats:
     - NETAPPDUMP
     - CELERRADUMP
     - NDMPDUMP
  2. Write data simultaneously to active-data pools is not supported when LAN-free data movement is used. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is accepted.
  3. The simultaneous-write function is not supported when a NAS backup operation is writing a TOC file. If the primary storage pool specified in the TOCDESTINATION in the copy group of the management class has active-data pools defined, the active-data pools are ignored, and the data is stored into the primary storage pool only.
  4. You cannot use the simultaneous-write function with CENTERA storage devices.
  5. Data being imported is not stored in active-data pools. After an import operation, use the COPY ACTIVEDATA command to store the imported data in an active-data pool.

  Attention: The function that is provided by the ACTIVEDATAPOOLS parameter is not intended to replace the COPY ACTIVEDATA command. If you use the ACTIVEDATAPOOLS parameter, use the COPY ACTIVEDATA command to ensure that the active-data pools contain all active data of the primary storage pool.

DEDUPlicate
: Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE-type device class. The default value is NO.

IDENTIFYPRocess
: Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. Enter a value 0 - 50. The default value is 1. If the value of the DEDUPLICATE parameter is NO, the default setting for IDENTIFYPROCESS has no effect.

Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Define a primary storage pool with an 8MMTAPE device class

Define a primary storage pool that is named 8MMPOOL to the 8MMTAPE device class (with a device type of 8MM) with a maximum file size of 5 MB. Store any files larger than 5 MB in subordinate pools, beginning with POOL1. Enable collocation of files for client nodes. Allow as many as 5 scratch volumes for this storage pool.

```
define stgpool 8mmpool 8mmtape maxsize=5m
 nextstgpool=pool1 collocate=node
 maxscratch=5
```

Related reference:
SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)

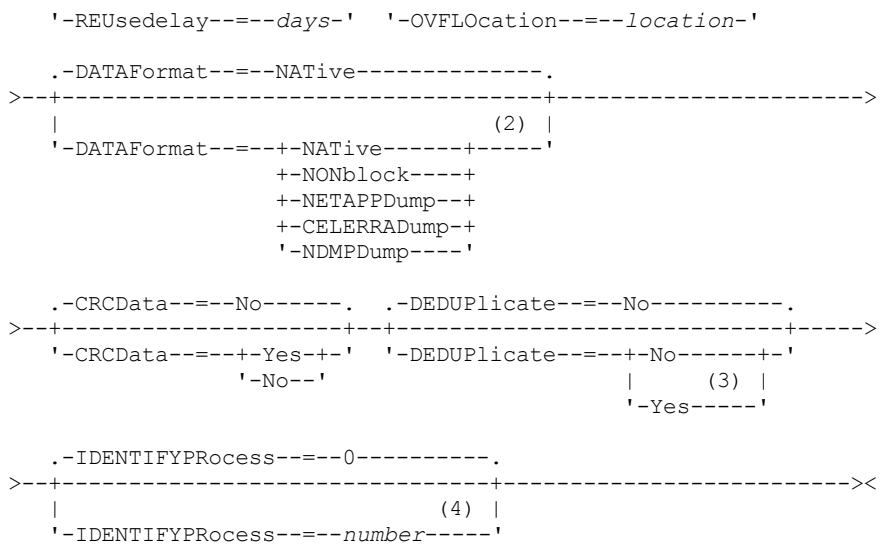
DEFINE STGPOOL (Define a copy storage pool assigned to sequential access devices)

Use this command to define a copy storage pool that is assigned to sequential access devices.

Privilege class

To issue this command, you must have system privilege.

Syntax



Notes:

1. The RECLAMATIONTYPE=SNAPLOCK setting is valid only for storage pools that are defined to servers that are enabled for IBM Spectrum Protect™ for Data Retention. The storage pool must be assigned to a FILE device class, and the directories that are specified in the device class must be NetApp SnapLock volumes.
2. The values NETAPPDUMP, CELERRADUMP, and NDMPDUMP are not valid for storage pools that are defined with a FILE device class.
3. This parameter is valid only for storage pools that are defined with a FILE device class.
4. This parameter is available only when the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
: Specifies the name of the storage pool to be defined. The name must be unique, and the maximum length is 30 characters.

device_class_name (Required)
: Specifies the name of the sequential access device class to which this copy storage pool is assigned. You can specify any device class except DISK.

POoltype=COpy (Required)
: Specifies that you want to define a copy storage pool.

DESCription
: Specifies a description of the copy storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

ACCess
: Specifies how client nodes and server processes (such as reclamation) can access files in the copy storage pool. This parameter is optional. The default value is READWRITE. You can specify the following values:

  READWrite
  : Specifies that files can be read from and written to the volumes in the copy storage pool.

  READOnly
  : Specifies that client nodes can read files that are stored only on the volumes in the copy storage pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the copy storage pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the copy storage pool from volumes outside the storage pool. A storage pool cannot be backed up to the copy storage pool.

  UNAVailable
  : Specifies that client nodes cannot access files that are stored on volumes in the copy storage pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the copy storage pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the copy storage pool from volumes outside the storage pool. A storage pool cannot be backed up to the copy storage pool.

COLlocate

Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

- A single client node
- A group of file spaces
- A group of client nodes
- A client file space

This parameter is optional. The default value is NO.

Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required.

You can specify one of the following options:

No
: Specifies that collocation is disabled.

GRoup
: Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

  If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

  For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

  - Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
  - Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.

  If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

  - Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
  - Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces named A, B, C, D, and E. File spaces A and B belong to a filespace collocation group but C, D, and E do not. File spaces A and B are collocated by filespace collocation group, while C, D, and E are collocated by node.

  Data is collocated on the least amount of sequential access volumes.

NODe
: Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

  If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

FIlespace
: Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

RECLaim

Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the IBM Spectrum Protect database.

Reclamation makes the fragmented space on volumes usable again by moving any remaining unexpired files from one volume to another volume, thus making the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100. The default value is 100, which means that reclamation is not completed.

The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

If you change the value from the default, specify a value of 50 percent or greater so that files stored on two volumes can be combined onto a single output volume.

When a copy pool volume that is offsite becomes eligible for reclamation, the reclamation process attempts to obtain the unexpired files on the reclaimable volume from a primary or copy storage pool that is onsite. The process then writes these files to an available volume in the original copy storage pool. Effectively, these files are moved back to the onsite location. However, the files can be obtained from the offsite volume after a disaster if a database backup is used that references the files on the offsite volume. Because of the way reclamation works with offsite volumes, use it carefully with copy storage pools.

RECLAIMPRocess
Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999. The default value is 1.
When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

- The number of sequential storage pools.
- The number of logical and physical drives that can be dedicated to the operation.

To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for the storage pools must have a mount limit of at least 16.

You can specify one or more reclamation processes for each copy storage pool. You can specify multiple concurrent reclamation processes for a single copy storage pool, which makes better use of your available tape drives or FILE volumes. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

RECLAMATIONType
Specifies the method by which volumes are reclaimed and managed. This parameter is optional. The default value is THRESHOLD. The following are possible values:

THRESHold
Specifies that volumes that belong to this storage pool are reclaimed based on the threshold value in the RECLAIM attribute for this storage pool.

SNAPlock
Specifies that FILE volumes that belong to this storage pool are managed for retention by using NetApp Data ONTAP software and NetApp SnapLock volumes. This parameter is only valid for storage pools that being defined to a server that has data retention protection that is enabled and that is assigned to a FILE device class. Volumes in this storage pool are not reclaimed based on threshold; the RECLAIM value for the storage pool is ignored.

All volumes in this storage pool are created as FILE volumes. A retention date, which is derived from the retention attributes in the archive copy group for the storage pool, is set in the metadata for the FILE volume by using the SnapLock feature of the NetApp Data ONTAP operating system. Until the retention date expires, the FILE volume and any data on it cannot be deleted from the physical SnapLock volume on which it is stored.

The RECLAMATIONTYPE parameter for all storage pools that are being defined must be the same when defined to the same device class name. The DEFINE command fails if the RECLAMATIONTYPE parameter specified is different from what is defined for storage pools that are already defined to the device class name.

OFFSITERECLAIMLimit
Specifies the number of offsite volumes that space is reclaimed from during reclamation for this storage pool. This parameter is optional. The default value is NOLIMIT. You can specify the following values:

NOLimit
Specifies that you want to reclaim the space in all of your offsite volumes.

number
Specifies the number of offsite volumes to reclaim space from. You can specify an integer 0 - 99999. A value of zero means that none of the offsite volumes are reclaimed.
Tip:

To determine the value for the OFFSITERECLAIMLIMIT, use the statistical information in the message that is issued at the end of the offsite volume reclamation operation. The statistical information includes the following items:

- The number of offsite volumes that were processed
- The number of parallel processes that were used
- The total amount of time required for the processing

The order in which offsite volumes are reclaimed is based on the amount of unused space in a volume. (Unused space includes both space that has never been used on the volume and space that has become empty because of file deletion.) Volumes with the largest amount of unused space are reclaimed first.

For example, suppose a copy storage pool contains three volumes: VOL1, VOL2, and VOL3. VOL1 has the largest amount of unused space, and VOL3 has the least amount of unused space. Suppose further that the percentage of unused space in each of the three volumes is greater than the value of the RECLAIM parameter. If you do not specify a value for the OFFSITERECLAIMLIMIT parameter, all three volumes will be reclaimed when the reclamation runs. If you specify a value of 2, only VOL1 and VOL2 will be reclaimed when the reclamation runs. If you specify a value of 1, only VOL1 will be reclaimed.

MAXSCRatch (Required)
Specifies the maximum number of scratch volumes that the server can request for this storage pool. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes as needed, you avoid having to define each volume to be used.

The value that is specified for this parameter is used to estimate the total number of volumes available in the copy storage pool and the corresponding estimated capacity for the copy storage pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. However, if the access mode for a scratch volume is OFFSITE, the volume is not deleted from the copy storage pool until the access mode is changed. An administrator can then query the server for empty, offsite scratch volumes and return them to the onsite location.

When scratch volumes with the device type of FILE become empty and are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay
Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. The default value is 0, which means that a volume can be rewritten or returned to the scratch pool as soon as all the files are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to files in the copy storage pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. The number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

OVFLOcation
Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.

DATAFormat

Specifies the data format to use to back up files to this storage pool and restore files from this storage pool. The default format is the NATIVE server format. You can specify the following values:

NATive
: Specifies the data format is the native IBM Spectrum Protect server format and includes block headers.

NONblock
: Specifies the data format is the native IBM Spectrum Protect server format and does not include block headers. The default minimum block size on a volume that is associated with a FILE device class is 256 KB, regardless how much data is written to the volume. For certain tasks, you can minimize wasted space on storage volumes by specifying the NONBLOCK data format. For example, you can specify the NONBLOCK data format for the following tasks:

  - Using content-management products
  - Using the DIRMC client option to store directory information
  - Migrating very small files by using IBM Spectrum Protect for Space Management or IBM Spectrum Protect HSM for Windows

  In most situations, however, the NATIVE format is preferred.

NETAPPDump
: Specifies that the data is in a NetApp dump format. Do not specify this data format for file system images that are in a dump format and that were backed up from a NetApp file server by using NDMP. The server does not complete storage pool reclamation or AUDIT VOLUME for a storage pool with DATAFORMAT=NETAPPDUMP. You can use the MOVE DATA command to move NDMP-generated data out of a volume if the volume must be reused.

CELERRADump
: Specifies that the data is in an EMC Celerra dump format. Do not specify this data format for file system images that are in a dump format and that were backed up from an EMC Celerra file server by using NDMP. The server does not complete storage pool reclamation or AUDIT VOLUME for a storage pool with DATAFORMAT=CELERRADUMP. You can use the MOVE DATA command to move NDMP-generated data out of a volume if the volume must be reused.

NDMPDump
: Specifies that the data is in a NAS vendor-specific backup format. Do not specify this data format for file system images that are in a backup format and that were backed up from a NAS file server other than a NetApp or EMC Celerra file server. The server does not complete storage pool reclamation or AUDIT VOLUME for a storage pool with DATAFORMAT=NDMPDUMP. You can use the MOVE DATA command to move NDMP-generated data out of a volume if the volume must be reused.

CRCData
: Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

  Yes
  : Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

  No
  : Specifies that data is stored without CRC information.

  Tip:

  For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

  To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

  - IBM® LTO5 and later.
  - IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
  - Oracle StorageTek T10000C and T10000D drives.

DEDUPlicate

Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE-type device class. The default value is NO.

IDENTIFYPRocess

Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. Enter a value 0 - 50.

The default value for this parameter is 0. Data-deduplication processes for a copy storage pool are not necessary if you specify data-deduplication processes for the primary storage pool. When IBM Spectrum Protect analyzes a file in a storage pool, IBM Spectrum Protect also analyzes the file in all other storage pools.

Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Define a copy storage pool with a DC480 device class.

Define a copy storage pool, TAPEPOOL2, to the DC480 device class. Allow up to 50 scratch volumes for this pool. Delay the reuse of volumes for 45 days.

```
define stgpool tapepool2 dc480 pooltype=copy
 maxscratch=50 reusedelay=45
```

Related reference:
SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)

DEFINE STGPOOL (Define an active-data pool assigned to sequential-access devices)

Use this command to define an active-data pool assigned to sequential-access devices.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
   '-RECLAMATIONType--=--+-THRESHold-+-----'
                         '-SNAPlock--'

   .-OFFSITERECLAIMLimit--=--NOLimit-.
>--+---------------------------------+--MAXSCRatch--=--number--->
   '-OFFSITERECLAIMLimit--=--number--'

   .-REUsedelay--=--0----.
>--+---------------------+--+-------------------------+-------->
   '-REUsedelay--=--days-'  '-OVFLOcation--=--location-'

   .-DATAFormat--=--NATive-------.  .-CRCData--=--No------.
>--+-----------------------------+--+---------------------+----->
   '-DATAFormat--=--+-NATive---+-'  '-CRCData--=--+-Yes-+-'
                    '-NONblock-'                  '-No--'

   .-DEDUPlicate--=--No----------.
>--+-----------------------------+----------------------------->
   '-DEDUPlicate--=--+-No------+-'
                     |     (2) |
                     '-Yes-----'

   .-IDENTIFYPRocess--=--0----------.
>--+-------------------------------+-------------------------><
   |                           (3) |
   '-IDENTIFYPRocess--=--number-----'
```

Notes:

1. The RECLAMATIONTYPE=SNAPLOCK setting is valid only for storage pools that are defined to servers that are enabled for IBM Spectrum Protect™ for Data Retention. The storage pool must be assigned to a FILE device class, and the directories that are specified in the device class must be NetApp SnapLock volumes.
2. This parameter is valid only for storage pools that are defined with a FILE device class.
3. This parameter is available only when the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
: Specifies the name of the storage pool to be defined. The name must be unique, and the maximum length is 30 characters.

device_class_name (Required)
: Specifies the name of the sequential access device class to which this active-data pool is assigned. You can specify any device class except DISK.

POoltype=ACTIVEdata (Required)
: Specifies that you want to define an active-data pool.

DESCription
: Specifies a description of the active-data pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

ACCess
: Specifies how client nodes and server processes (such as reclamation) can access files in the active-data pool. This parameter is optional. The default value is READWRITE. You can specify the following values:

  READWrite
  : Specifies that files can be read from and written to the volumes in the active-data pool.

  READOnly
  : Specifies that client nodes can read only files that are stored on the volumes in the active-data pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the active-data pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the active-data pool from volumes outside the storage pool. A storage pool cannot be copied to the active-data pool.

  UNAVailable
  : Specifies that client nodes cannot access files that are stored on volumes in the active-data pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the active-data pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the active-data pool from volumes outside the storage pool. A storage pool cannot be copied to the active-data pool.

COLlocate

Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

- A single client node
- A group of file spaces
- A group of client nodes
- A client file space

This parameter is optional. The default value is NO.

Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required.

You can specify one of the following options:

No

Specifies that collocation is disabled.

GRoup

Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
- Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.

If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
- Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces named A, B, C, D, and E. File spaces A and B belong to a filespace collocation group but C, D, and E do not. File spaces A and B are collocated by filespace collocation group, while C, D, and E are collocated by node.

Data is collocated on the least amount of sequential access volumes.

NODe

Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

FIlespace

Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

RECLaim

Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the IBM Spectrum Protect database.

Reclamation makes the fragmented space and space occupied by inactive backup files on volumes usable again by moving any remaining unexpired files and active backup files from one volume to another volume. This action makes the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100. The default value is 60.

The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

If you change the value from the default, specify a value of 50 percent or greater so that files stored on two volumes can be combined onto a single output volume.

When an active-data pool volume that is offsite becomes eligible for reclamation, the reclamation process attempts to obtain the unexpired files on the reclaimable volume from a primary or active-data pool that is onsite. The process then writes these files to an available volume in the original active-data pool. Effectively, these files are moved back to the onsite location. However, the files can be obtained from the offsite volume after a disaster if a database backup is used that references the files on the offsite volume. Because of the way reclamation works with offsite volumes, use it carefully with active-data pools.

RECLAIMPRocess
Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999. The default value is 1.
When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

- The number of sequential storage pools.
- The number of logical and physical drives that can be dedicated to the operation.

To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for the storage pools must have a mount limit of at least 16.

You can specify one or more reclamation processes for each active-data pool. You can specify multiple concurrent reclamation processes for a single active-data pool, which makes better use of your available tape drives or FILE volumes. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

RECLAMATIONType
Specifies the method by which volumes are reclaimed and managed. This parameter is optional. The default value is THRESHOLD. The following are possible values:

THRESHold
Specifies that volumes that belong to this storage pool are reclaimed based on the threshold value in the RECLAIM attribute for this storage pool.

SNAPlock
Specifies that FILE volumes that belong to this storage pool are managed for retention by using NetApp Data ONTAP software and NetApp SnapLock volumes. This parameter is only valid for storage pools that are being defined to a server that has data retention protection that is enabled and that is assigned to a FILE device class. Volumes in this storage pool are not reclaimed based on threshold; the RECLAIM value for the storage pool is ignored.

All volumes in this storage pool are created as FILE volumes. A retention date, which is derived from the retention attributes in the archive copy group for the storage pool, is set in the metadata for the FILE volume by using the SnapLock feature of the NetApp Data ONTAP operating system. Until the retention date expires, the FILE volume and any data on it cannot be deleted from the physical SnapLock volume on which it is stored.

The RECLAMATIONTYPE parameter for all storage pools that are being defined must be the same when defined to the same device class name. The DEFINE command fails if the RECLAMATIONTYPE parameter specified is different from what is defined for storage pools that are already defined to the device class name.

OFFSITERECLAIMLimit
Specifies the number of offsite volumes that space is reclaimed from during reclamation for this storage pool. This parameter is optional. The default value is NOLIMIT. You can specify the following values:

NOLimit
Specifies that you want to reclaim the space in all of your offsite volumes.

number
Specifies the number of offsite volumes to reclaim space from. You can specify an integer 0 - 99999. A value of zero means that none of the offsite volumes are reclaimed.
Tip:

To determine the value for the OFFSITERECLAIMLIMIT, use the statistical information in the message that is issued at the end of the offsite volume reclamation operation. The statistical information includes the following items:

- The number of offsite volumes that were processed
- The number of parallel processes that were used
- The total amount of time required for the processing

The order in which offsite volumes are reclaimed is based on the amount of unused space in a volume. (Unused space includes both space that has never been used on the volume and space that has become empty because of file deletion.) Volumes with the largest amount of unused space are reclaimed first.

For example, suppose an active-data pool contains three volumes: VOL1, VOL2, and VOL3. VOL1 has the largest amount of unused space, and VOL3 has the least amount of unused space. Suppose further that the percentage of unused space in each of the three volumes is greater than the value of the RECLAIM parameter. If you do not specify a value for the OFFSITERECLAIMLIMIT parameter, all three volumes are reclaimed when the reclamation runs. If you specify a value of 2, only VOL1 and VOL2 are reclaimed when the reclamation runs. If you specify a value of 1, only VOL1 is reclaimed.

MAXSCRatch (Required)
Specifies the maximum number of scratch volumes that the server can request for this storage pool. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes as needed, you avoid having to define each volume to be used.

The value that is specified for this parameter is used to estimate the total number of volumes available in the active-data pool and the corresponding estimated capacity for the active-data pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. However, if the access mode for a scratch volume is OFFSITE, the volume is not deleted from the active-data pool until the access mode is changed. An administrator can then query the server for empty, offsite scratch volumes and return them to the onsite location.

When scratch volumes with the device type of FILE become empty and are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay
Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. The default value is 0, which means that a volume can be rewritten or returned to the scratch pool as soon as all the files are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to files in the active-data pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. The number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

OVFLOcation
Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.

DATAFormat

Specifies the data format to use to copy files to this storage pool and restore files from this storage pool. The default format is the NATIVE server format. You can specify the following values:

NATive
: Specifies the data format is the native IBM Spectrum Protect server format and includes block headers.

NONblock
: Specifies the data format is the native IBM Spectrum Protect server format and does not include block headers. The default minimum block size on a volume that is associated with a FILE device class is 256 KB, regardless how much data is written to the volume. For certain tasks, you can minimize wasted space on storage volumes by specifying the NONBLOCK data format. For example, you can specify the NONBLOCK data format for the following tasks:

  - Using content-management products
  - Using the DIRMC client option to store directory information
  - Migrating very small files by using IBM Spectrum Protect for Space Management or IBM Spectrum Protect HSM for Windows

  In most situations, however, the NATIVE format is preferred.

CRCData
: Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

  Yes
  : Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

  No
  : Specifies that data is stored without CRC information.

  Tip:

  For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

  To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

  - IBM® LTO5 and later.
  - IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
  - Oracle StorageTek T10000C and T10000D drives.

DEDUPlicate
: Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. The default value is NO.

IDENTIFYPRocess
: Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. Enter a value 0 - 50.

  The default value for this parameter is 0. Data-deduplication processes for a copy storage pool are not necessary if you specify data-deduplication processes for the primary storage pool. When IBM Spectrum Protect analyzes a file in a storage pool, IBM Spectrum Protect also analyzes the file in all other storage pools.

  Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Define an active-data pool with a DC500 device class

Define an active-data pool, TAPEPOOL2, to the DC500 device class. Allow up to 50 scratch volumes for this pool. Delay the reuse of volumes for 45 days.

```
define stgpool tapepool3 dc500 pooltype=activedata
 maxscratch=50 reusedelay=45
```

Related reference:
SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)

DEFINE STGPOOLDIRECTORY (Define a storage pool directory)

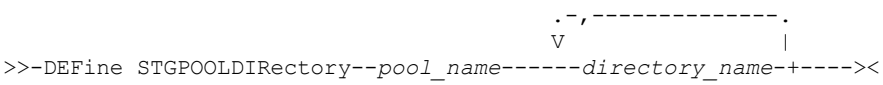
Use this command to define one or more directories in a directory-container or cloud-container storage pool.

Tip: After you define a cloud-container storage pool, create one or more directories that are used for local storage. You can temporarily store data in local storage during the data ingestion, before the data is moved to the cloud. In this way, you can improve backup and archive performance. For more information, see Optimizing performance for cloud object storage.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

pool_name (Required)
: Specifies the name of a directory-container or cloud-container storage pool. This parameter is required.

directory_name (Required)
: Specifies the directory to be defined in the storage pool. This parameter is required. You can specify more than one directory name by separating each name with a comma, with no intervening spaces.

  If you use the administrative client and the directory name contains a comma or a backslash ("\"), enclose the name in quotation marks.

Example: Define a storage pool directory

Define a storage pool directory that is named DIR1 by using a directory-container storage pool that is named POOL1.

AIX | Linux

```
define stgpooldirectory pool1 /storage/dir1
```

Windows

```
define stgpooldirectory pool1 c:\storage\dir1
```

Example: Define multiple storage pool directories

Define storage pool directories that are named DIR1 and DIR2 by using a directory-container storage pool that is named POOL1.

AIX | Linux

```
define stgpooldirectory pool1 /storage/dir1,/storage/dir2
```

Windows

```
define stgpooldirectory pool1 e:\storage\dir1,f:\storage\dir2
```

Example: Define local storage for a cloud-container storage pool

Create a storage pool directory that is named DIR3 in a cloud-container storage pool that is named CLOUDLOCALDISK1.

AIX Linux

```
define stgpooldirectory cloudlocaldisk1 /storage/dir3
```

Windows

```
define stgpooldirectory cloudlocaldisk1 c:\storage\dir3
```

Table 1. Commands related to DEFINE STGPOOLDIRECTORY

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE STGPOOLDIRECTORY	Deletes a storage pool directory from a directory-container or cloud-container storage pool.
QUERY STGPOOLDIRECTORY	Displays information about storage pool directories.
UPDATE STGPOOLDIRECTORY	Changes the attributes of a storage pool directory.

DEFINE STGRULE (Define a storage rule)

Use this command to define a storage rule.

The DEFINE STGRULE command takes several forms. The syntax and parameters for each form are defined separately.

Table 1. Commands related to DEFINE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (auditing)	Updates a storage rule for auditing storage pools.
UPDATE STGRULE (data deduplication statistics)	Updates a storage rule for generating data deduplication statistics.
UPDATE STGRULE (reclaiming)	Updates a storage rule for reclaiming cloud-container storage pools.
UPDATE STGRULE (tiering)	Updates a tiering storage rule.

- DEFINE STGRULE (Define a rule for auditing storage pools)
  Use this command to schedule audit operations for a storage pool. The audit operations are designed to identify corrupted files within the storage pool.
- DEFINE STGRULE (Define a rule for generating data deduplication statistics)
  Use this command to define a rule for generating data deduplication statistics. You can define one or more storage rules for a target container storage pool.
- DEFINE STGRULE (Define a rule for reclaiming cloud containers)
  Use this command to define a rule for daily space reclamation in cloud-container storage pools. You can define one storage rule per storage pool.
- DEFINE STGRULE (Define a storage rule for tiering)
  Use this command to define a storage rule for one or more storage pools. The storage rule schedules tiering between container storage pools. You can define one or more storage rules for a target container storage pool.

DEFINE STGRULE (Define a rule for auditing storage pools)

Use this command to schedule audit operations for a storage pool. The audit operations are designed to identify corrupted files within the storage pool.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine STGRULE--rule_name--storage_pool---------------------->

                              .-DELAY--=--7-----.
>----ACTiontype--=--AUDit----+-----------------+---------------->
                              '-DELAY--=--delay-'

   .-AUDITType--=--Extent-.  .-AUDITLevel--=--5-----.
>--+--------------------+--+--------------------+----------->
                              '-AUDITLevel--=--+-1-+-'
                                               '-5-'

   .-STARTTime--=--current_time-.  .-ACTIVE--=--Yes-----.
>--+-----------------------------+--+--------------------+------->
   '-STARTTime--=--time---------'  '-ACTIVE--=--+-No--+-'
                                               '-Yes-'

>--+---------------------------+---------------------------><
   '-DESCription--=--description-'
```

Parameters

rule_name (Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

storage_pool (Required)
: Specifies the name of the storage pool to audit.

ACTiontype=AUDit (Required)
: Specifies that the storage rule is for an audit operation.

DELAY
: Specifies the interval, in days, between audit operations. This parameter is optional. The default value is 7 days. You can specify an integer in the range 1 - 9999.

AUDITType
: Specifies the audit type. This parameter is optional. You can specify the following value:

  Extent
  : Specifies that only extents are audited. This is the default value.
    Restriction: In IBM Spectrum Protect™ Version 8.1.5, you can use the DEFINE STGRULE command with the ACTIONTYPE=AUDIT setting only to audit extents. Objects are not audited.

AUDITLevel
: Specifies the level of the audit. This parameter is optional. The following values are possible:

  1
  : Specifies a minimal audit operation of the extents in the storage pool.

  5
  : Specifies a full audit operation of the extents in the storage pool. This is the default value.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. The default is the current time. This parameter is optional.
  You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE

Specifies whether storage rule processing occurs. This parameter is optional. The default is YES. The following values are possible:

Yes
: Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

No
: Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

DESCription
: Specifies a description of the storage rule. This parameter is optional. The maximum length of the description is 255 characters. If the description includes spaces, enclose the description in quotation marks.

Define a rule for an extent-level audit operation

Define a storage rule, FULLAUDIT, to schedule a full audit of extents in storage pool DIRPOOL. The audit operation is started now and is repeated every three days:

```
define stgrule fullaudit dirpool actiontype=audit delay=3 auditlevel=5 starttime=now
```

Related commands

Table 1. Commands related to DEFINE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (auditing)	Updates a storage rule for auditing storage pools.

DEFINE STGRULE (Define a rule for generating data deduplication statistics)

Use this command to define a rule for generating data deduplication statistics. You can define one or more storage rules for a target container storage pool.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>--+-------------------------+---------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-FSList--=--*----------------------.
>--+-----------------------------------+---------------------->
   |            .-,------------------. |
   |            V                    | |
   '-FSList--=----+-filespace_name-+-+-'
                  +-,--------------+
                  '-fsid-----------'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+------------------------------>
   '-CODEType--=--+-UNIcode----+-'
                  +-NONUNIcode-+
                  '-BOTH-------'

>--+-----------------------------+------------------------------><
   '-DESCription--=--description-'
```

Parameters

rule_name (Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

target_stgpool (Required)
: Specifies the name of the target storage pool.

ACTiontype=GENdedupstats (Required)
: Specifies that data deduplication statistics are generated.

DELAY
: Specifies the interval, in days, between operations to collect statistics. The default value is 1 day. You can specify an integer in the range 0 - 9999.

MAXProcess
: Specifies the maximum number of parallel processes to collect statistics. This parameter is optional. You can enter a value in the range 1 - 99. The default value is 8. For example, if you have 4 storage pools and you specify the default value for this parameter, 32 processes are started.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. The default is the current time. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.
You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
: Specifies whether the storage rule processing occurs. This parameter is optional. The default is YES. The following values are possible:

  No
  : Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

  Yes
  : Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

NODEList
: Specifies the name of the client node or defined group of client nodes for which data deduplication statistics are collected. You can also specify a combination of client node names and client-node group names. To specify multiple client node names or client-node group names, separate the names with commas with no intervening spaces. You can use wildcard

characters with client node names but not with client-node group names. The specified value can have a maximum of 1024 characters. The default value is an asterisk (*), which shows information for all client nodes.

NAMEType
Specifies how you want the server to interpret the file space names that you enter. Use this parameter when IBM Spectrum Protect™ clients have file spaces that are in Unicode format, and are on Windows, NetWare, or Macintosh OS X operating systems. This parameter is optional.
This parameter is required if you specify a node name and a file space name or FSID.
Restriction: When you specify this parameter, the file space name cannot contain an asterisk.

Specify one of the following values:

SERVER
The server uses the server's code page to interpret the file space names. This is the default.
UNIcode
The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the characters in the name and the server's code page.
Tip: Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.
FSID
The server interprets the file space names as their FSIDs.

FSList
Specifies the names of one or more file spaces for which data deduplication statistics are collected. This parameter is optional. You can use wildcard characters to specify this name. The specified value can have a maximum of 1024 characters. An asterisk is the default. You can specify one of the following values:

*
Specify an asterisk (*) to show information for all file spaces or IDs.
filespace_name
Specifies the name of the file space. You can specify more than one file space by separating the names with commas and no intervening spaces.
fsid
Specifies the name of a file space identifier. This parameter is valid for clients with file spaces that are in Unicode format. Specify more than one file space by separating the names with commas and no intervening spaces.

For clients with file spaces that are in Unicode format, you can enter either a file space name or an FSID. If you enter a file space name, the server might have to convert the file space name that you enter. For example, the server might have to convert the name that you enter from the server's code page to Unicode.
Restrictions: The following restrictions apply to file space names and FSIDs:

- You must specify a node name if you specify a file space name.
- Do not specify both file space names and FSIDs on the same command.

CODEType
Specifies what type of file spaces to include in the record. The default value is BOTH, which specifies that file spaces are included regardless of code page type. Use this parameter only when you enter an asterisk to display information about all file spaces. This parameter is optional. Specify one of the following values:

UNIcode
Include file spaces that are in Unicode format.
NONUNIcode
Include file spaces that are not in Unicode format.
BOTH
Include file spaces regardless of code page type. This is the default.

DESCription
Specifies a description of the storage rule. This parameter is optional.

Define a rule to generate data deduplication statistics

Define a storage rule that is named MYSTAT1 to generate data deduplication statistics for the target storage pool, TARGET1. Limit the scope to a node that is named NODE1 and to the MYNODEGROUP node group. Limit the file spaces to FS1 and to all file spaces whose names start with FILESPACE1:

```
define stgrule mystat1 target1 actiontype=gendedupstats
nodelist=node1,mynodegroup fslist=/fs1,/filespace1*
```

Related commands

Table 1. Commands related to DEFINE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (data deduplication statistics)	Updates a storage rule for generating data deduplication statistics.

DEFINE STGRULE (Define a rule for reclaiming cloud containers)

Use this command to define a rule for daily space reclamation in cloud-container storage pools. You can define one storage rule per storage pool.

Privilege class

To issue this command, you must have system privilege.
Restriction: You can configure a cloud reclamation rule for a storage pool only on a Microsoft Azure cloud computing system or on a cloud computing system with the Simple Storage Service (S3) protocol.

Syntax

```
>>-DEFine STGRULE--rule_name--pool_name------------------------>

                                .-PCTUnused--=--70---------.
>----ACTiontype--=--REClaim----+--------------------------+----->
                                '-PCTUnused--=--percentage-'

   .-MAXPRocess--=--16-----.  .-DUration--=--120-----.
>--+----------------------+--+---------------------+---------->
   '-MAXPRocess--=--number-'  '-DUration--=--minutes-'

   .-STARTTime--=--current_time-.  .-ACTIVE--=--Yes-----.
>--+----------------------------+--+-------------------+------->
   '-STARTTime--=--time---------'  '-ACTIVE--=--+-No--+-'
                                               '-Yes-'

>--+----------------------------+---------------------------><
   '-DESCription--=--description-'
```

Parameters

rule_name (Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

pool_name (Required)
: Specifies the name of the cloud-container storage pool.

ACTiontype=REClaim (Required)
: Specifies that a cloud-container storage pool is reclaimed. Used data extents are moved to a new container. Unused extents are discarded.

PCTUnused
: Specifies the percentage of the container that is no longer in use. After unused space reaches a percentage that you designate, the cloud container is reclaimed. The default value is 70 percent. You can specify an integer in the range 50 - 99. This parameter is optional.

MAXProcess
: Specifies the maximum number of parallel processes that can be used to complete the storage rule for the storage pool that is specified. This parameter is optional. You can enter a value in the range 1 - 99. The default value is 16.

DUration

Specifies the maximum number of minutes that the storage rule runs before it is automatically canceled. You can specify a number in the range 60 - 1440. The default value is 120 minutes (2 hours). This parameter is optional.

STARTTime

Specifies the time for the beginning of the window in which the storage rule is first processed. The default is the current time. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.

You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE

Specifies whether the storage rule processing occurs. This parameter is optional. The default is YES. The following values are possible:

No

Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

Yes

Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

DESCription

Specifies a description of the storage rule. This parameter is optional.

Define a rule to reclaim space in a cloud-container storage pool

Define a storage rule that is named RECLAIMCTR1 to reclaim cloud containers that are more than half unused in storage pool CLOUDPOOL1. Specify a start time of 04:00 hours with a maximum of 2 processes for the storage rule:

```
define stgrule reclaimctr1 cloudpool1 actiontype=reclaim
pctunused=51 maxprocess=2 starttime=04:00:00
```

Related commands

Table 1. Commands related to DEFINE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (reclaiming)	Updates a storage rule for reclaiming cloud-container storage pools.

DEFINE STGRULE (Define a storage rule for tiering)

Use this command to define a storage rule for one or more storage pools. The storage rule schedules tiering between container storage pools. You can define one or more storage rules for a target container storage pool.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine STGRULE--rule_name--target_stgpool-------------------->

                              .-,------------------------.
                              V                          |
```

```
>----ACTiontype--=--Tier--------SRCPools--=--source_pool-+------>

   .-TIERDelay--=--30----.  .-MAXPRocess--=--8------.
>--+--------------------+--+----------------------+----------->
   '-TIERDelay--=--delay-'  '-MAXPRocess--=--number-'

   .-DURation--=--NOLimit-.  .-STARTTime--=--current_time-.
>--+--------------------+--+-------------------------+----->
   '-DURation--=--minutes-'  '-STARTTime--=--time---------'

   .-ACTIVE--=--Yes-----.
>--+--------------------+--+---------------------------+-----><
   '-ACTIVE--=--+-No--+-'  '-DESCription--=--description-'
                '-Yes-'
```

Parameters

rule_name(Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

target_stgpool(Required)
: Specifies the name of the target cloud-container storage pool.

ACTiontype=Tier(Required)
: Specifies that the storage rule tiers objects from the source storage pool to the target storage pool.

  You can use tiering to lower storage costs by moving data to a cloud-container storage pool.

SRCPools(Required)
: Specifies the name of the source directory-container storage pools. If you specify a pool as the source of a storage rule, you cannot specify the same pool as the source of another storage rule. To specify multiple storage pools, separate the names with commas with no intervening spaces. You must specify this parameter if the ACTIONTYPE=TIER parameter is specified.

TIERDelay
: Specifies the number of days to wait before the storage rule tiers objects to the next storage pool. The default value is 30 days. You can specify an integer in the range 0 - 9999. The parameter value applies to all files in the storage pool.

MAXProcess
: Specifies the maximum number of parallel processes to complete the storage rule for each source storage pool that is specified. This parameter is optional. Enter a value in the range 1 - 99. The default value is 8. For example, if you have 4 source storage pools and you specify the default value for this parameter, 32 processes are started.

DUration
: Specifies the maximum number of minutes that the storage rule runs before it is automatically canceled. You can specify a number in the range 60 - 1440. The default value is unlimited. If you do not specify a value, or if you specify a value of NOLimit, the storage rule runs until it is completed. This parameter is optional.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. The default is the current time. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.
  Specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
: Specifies whether the storage rule processing occurs. This parameter is optional. The default is YES. The following values are possible:

  No
  : Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

  Yes
  : Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

DESCription

Specifies a description of the storage rule. This parameter is optional.

Define a storage rule

Define a storage rule that is named tieraction to move data from the source directory-container storage pools dirpool1 and dirpool2 to the target cloud-container storage pool cloudpool1. Specify a start time of 03:00 hours that uses a maximum of 10 processes for a tiering storage rule:

```
define stgrule tieraction cloudpool1 srcpools=dirpool1,dirpool2
actiontype=tier maxprocess=10 starttime=03:00:00
```

Related commands

Table 1. Commands related to DEFINE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (tiering)	Updates a tiering storage rule.

DEFINE SUBSCRIPTION (Define a profile subscription)

Use this command on a managed server to subscribe that managed server to a profile.

When a server subscribes to its first profile, a subscription is also created to the default profile (if one exists) of the configuration manager. The server then contacts the configuration manager periodically for configuration updates.

Restrictions:

1. A server cannot subscribe to profiles from more than one configuration manager.
2. If a server subscribes to a profile with an associated object that is already defined on the server, the local definition is replaced by the definition from the configuration manager. For example, if a server has an administrative schedule named WEEKLY_ BACKUP, then subscribes to a profile that also has an administrative schedule named WEEKLY_BACKUP, the local definition is replaced.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DEFine SUBSCRIPtion--profile_name---------------------------->

>--+------------------------+---------------------------------><
   '-SERVer--=--server_name-'
```

Parameters

profile_name (Required)
: Specifies the name of the profile to which the server subscribes.

SERVer
: Specifies the name of the configuration manager from which the configuration information is obtained. This parameter is required, if the managed server does not have at least one subscription. If the managed server has a subscription, you can omit this parameter and it defaults to the configuration manager for that subscription.

Example: Define a profile subscription

Subscribe a profile named BETA that resides on a configuration manager named TOM.

```
define subscription beta server=tom
```

Related commands

Table 1. Commands related to DEFINE SUBSCRIPTION

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFILE	Deletes a profile from a configuration manager.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
LOCK PROFILE	Prevents distribution of a configuration profile.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY PROFILE	Displays information about configuration profiles.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.
SET CONFIGREFRESH	Specifies a time interval for managed servers to contact configuration managers.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

DEFINE VIRTUALFSMAPPING (Define a virtual file space mapping)

Use this command to define a virtual file space mapping.

Virtual file space names can be used in the NAS data operations BACKUP NODE and RESTORE NODE similar to a file system name. Refer to the documentation about your NAS device for guidance on specifying the parameters for this command.
Note: The NAS node must have an associated data mover definition because when the IBM Spectrum Protect™ server updates a virtual file space mapping, the server attempts to contact the NAS device to validate the virtual file system and file system name.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege
- Restricted policy privilege for the domain to which the NAS node is assigned.

Syntax

```
>>-DEFine VIRTUALFSmapping  -node_name-------------------------->

>--virtual_filespace_name--file_system_name--path--------------->

   .-NAMEType--=--SERVER----------.
>--+-----------------------------+--------------------------><
   '-NAMEType--=--+-SERVER------+-'
                  '-HEXadecimal-'
```

Parameters

node_name (Required)

Specifies the NAS node on which the file system and path reside. You cannot use wildcard characters or specify a list of names.

virtual_filespace_name (Required)

Specifies the name which refers to this virtual file space definition. The virtual file space name is case sensitive and the first character must be a forward slash /. The length of the name cannot be more than 64 characters, including the required forward slash. Virtual file space names are restricted to the same character set as all other objects in the server except that the forward slash / character is also allowed.

The virtual file space name cannot be identical to any file system on the NAS node. When selecting a virtual file space name, consider the following restrictions:

- If a file system is created on the NAS device with the same name as a virtual file system, a name conflict will occur on the server when the new file space is backed up. Use a string for the virtual file space name that is unlikely to be used as a real file system name on your NAS device in the future.

  For example: A user follows a naming convention for creating file spaces on a NAS device with names of the form /vol1, /vol2, /vol3. The user defines a virtual file space to the server with the name /vol9. If the user continues to use the same naming convention, the virtual file space name is likely to conflict with a real file space name at some point in the future.

- During backup and restore operations, the server verifies that a name conflict does not occur prior to starting the operation.
- The virtual file space name appears as a file space in the output of the QUERY FILESPACE command, and also in the backup and restore panels of the IBM Spectrum Protect web client. Therefore, consider selecting a name that unambiguously identifies this object as a directory path on the NAS device.

file_system_name (Required)

Specifies the name of the file system in which the path is located. The file system name must exist on the specified NAS node. The file system name cannot contain wildcard characters.

path (Required)

Specifies the path from the root of the file system to the directory. The path can only reference a directory. The maximum length of the path is 1024 characters. The path name is case sensitive.

NAMEType

Specifies how the server should interpret the path name specified. This parameter is useful when a path contains characters that are not part of the code page in which the server is running. The default value is SERVER.

Possible values are:

SERVER
: The server uses the server code page to interpret the path name.

HEXadecimal
: The server interprets the path that you enter as the hexadecimal representation of the path. This option should be used when a path contains characters that cannot be entered. This could occur if the NAS file system is set to a language different from the one in which the server is running.

Example: Define a virtual file space mapping

Define the virtual file space mapping name /mikeshomedir for the path /home/mike on the file system /vol/vol1 on the NAS node named NAS1.

```
define virtualfsmapping nas1 /mikeshomedir /vol/vol1 /home/mike
```

Related commands

Table 1. Commands related to DEFINE VIRTUALFSMAPPING

Command	Description
DELETE VIRTUALFSMAPPING	Delete a virtual file space mapping.
QUERY VIRTUALFSMAPPING	Query a virtual file space mapping.

Command	Description
UPDATE VIRTUALFSMAPPING	Update a virtual file space mapping.

DEFINE VOLUME (Define a volume in a storage pool)

Use this command to assign a random or sequential access volume to a storage pool.

When you define a random-access (DISK) storage-pool volume or a sequential access storage pool volume that is associated with a FILE device class, you can have the server create the volume before it is assigned. Alternatively, you can use space triggers to create preassigned volumes when predetermined space-utilization thresholds are exceeded. For details about space triggers, see DEFINE SPACETRIGGER (Define the space trigger). For volumes associated with device classes other than DISK or device types other than FILE, you can use the DEFINE VOLUME command to assign an already-created volume to a storage pool.

AIX Linux When you use a FILE device class for storage that is managed by a z/OS® media server, it is not necessary to format or define volumes. If you define a volume for such a FILE device class by using the DEFINE VOLUME command, the z/OS media server does not allocate space for the volume until the volume is opened for its first use.

Attention: Volumes for the z/OS media server that are created using the DEFINE VOLUME command remain physically full or allocated after the server empties the volume, for example, after expiration or reclamation. For FILE volumes, the DASD space is not relinquished to the system when the volume is emptied. If a storage pool requires an empty or filling volume, the FILE volume can be used. In contrast, tape volumes that are logically empty are the same as physically empty. FILE and tape volumes remain defined in the server. In contrast, SCRATCH volumes, including the physical storage that is allocated for SCRATCH FILE volumes, are returned to the system when emptied.

To create space in sequential access storage pools, you can define volumes or allow the server to request scratch volumes as needed, as specified by the MAXSCRATCH parameter for the storage pool. For storage pools associated with the FILE device class, the server can create private volumes as needed using storage-pool space triggers. For DISK storage pools, the scratch mechanism is not available. However, you can create space by creating volumes and then defining them to the server. Alternatively, you can have the server create volumes that use storage-pool space triggers.

The server does not validate the existence of a volume name when defining a volume in a storage pool that is associated with a library. The defined volume has "0" EST capacity until data is written to the volume.

Attention: The size of a storage pool volume cannot be changed after it is defined to the server.

AIX If you change the size of IBM Spectrum Protect™ volumes by extending raw logical volumes through SMIT or otherwise altering the file sizes of the volumes with operating system commands or utilities, the server might not initialize correctly and data can be lost.

Windows If you change the size of volumes by altering the file sizes of the volumes with operating system commands or utilities, the server might not initialize correctly and data can be lost.

Restrictions:

- You cannot use this command to define volumes in storage pools with the parameter setting `RECLAMATIONTYPE=SNAPLOCK`. Volumes in this type of storage pool are allocated by using the MAXSCRATCH parameter on the storage pool definition.
- You cannot define volumes in a storage pool that is defined with the CENTERA device class.
- Linux You cannot use raw logical volumes for storage pool volumes.

Physical files that are allocated with DEFINE VOLUME command are not removed from a file space if you issue the DELETE VOLUME command.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to which the volume is assigned.

Syntax

```
>>-DEFine Volume--pool_name--volume_name------------------------>
```

```
   .-ACCess--=--READWrite-------.
>--+----------------------------+-------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                +-UNAVailable-+
                |         (1) |
                '-OFfsite-----'

>--+-------------------------------------------------+----------->
   |                            .-Wait--=--No------. |
   '-Formatsize--=--megabytes--+------------------+-'
                               '-Wait--=--+-No--+-'
                                          '-Yes-'

   .-Numberofvolumes--=--1----------.
>--+-------------------------------+--------------------------->
   |                 (2)           |
   '-Numberofvolumes------=--number-'

>--+---------------------------+-------------------------------><
   |          (3)              |
   '-LOcation------=--location-'
```

Notes:

1. This value is valid only for volumes that are assigned to copy storage pools.
2. This parameter is valid only for DISK or FILE volumes.
3. This parameter is valid only for sequential access volumes.

Parameters

pool_name (Required)
: Specifies the name of the storage pool to which the volume is assigned.

volume_name (Required)
: Specifies the name of the storage pool volume to be defined. If you specify a number greater than 1 for the NUMBEROFVOLUMES parameter, the volume name is used as a prefix to generate multiple volume names. The volume name that you specify depends on the type of device that the storage pool uses.

  Each volume that is used by a server for any purpose must have a unique name. This requirement applies to all volumes, whether the volumes are used for storage pools, or used for operations such as database backup or export. The requirement also applies to volumes that reside in different libraries but that are used by the same server.

  AIX Linux Remember: Volume names cannot contain embedded blanks or equal signs.
  Windows Remember: Volume names cannot contain embedded blanks or equal signs, except for DISK or FILE volumes.
  See the following tables for volume name requirements:

  - Table 1: DISK
  - Table 2: FILE
  - AIX Linux Table 3: FILE for the z/OS media server
  - Table 4: Tape
  - AIX Linux Table 5: Tape for z/OS media server
  - Table 6: REMOVABLEFILE

Table 1. Volume name requirements for DISK

Volume Name Requirements	Example

Volume Name Requirements	Example

The name of the file to contain the volume data, with either the fully qualified path name or a path name relative to the current working directory.
 	
Windows If a name contains embedded blanks, equal signs, or other special characters, enclose the list in quotation marks.
	AIX Linux
	
	`/usr/storage/sbkup01.dsm`
	
	AIX If you are using an AIX® logical volume, enter the path name as:
	
	`/dev/rxxx`
	
	where xxx is the logical volume name.
	Windows
	
	`"c:\program files\tivoli\tsm\server\data3.dsm"`

Table 2. Volume name requirements for FILE

Volume Name Requirements	Example

The name of the file to contain the volume data, with either the fully qualified path name or the path name relative to a directory identified in the DIRECTORY parameter for the device class.
 	
Windows If a name contains embedded blanks, equal signs, or other special characters, enclose the list in quotation marks.
 	
Place FILE volumes in one of the directories that are specified with the DIRECTORY parameter of the DEFINE DEVCLASS command. Otherwise, storage agents might not have access to the volumes. For details, see DEFINE PATH (Define a path).
	AIX Linux
	
	`/data/fpool01.dsm`
	
	Windows
	
	`"f:\data storage\fpool01.dsm"`

AIX Linux

Table 3. z/OS media server: Volume name requirements for FILE

Volume Name Requirements	Example

Volume Name Requirements	Example
For FILE volumes used with the z/OS media server server, specify a data set name. The data set name can consist of one or more qualifiers that are delimited by a period. The qualifiers can contain up to 8 characters. The maximum length of the data set name is 44 characters. The first letter of each qualifier must be alphabetic or national (@#$), followed by alphabetic, national, hyphen, or numeric characters. To allocate the associated VSAM Linear Dataset when the volume is tendered on the z/OS system, the High Level Qualifier (HLQ) is typically filtered by specific ACS routines within the SMS policy constraints on the system where the z/OS media server is running. The behavior of the HLQ is similar to the behavior of the PREFIX name on a scratch request. The HLQ is typically used by DFSMS to affect allocation attributes, such as Extended Addressability for data sets that are expected to extend when space that is already allocated to the file volume is used up. If the data set does not exist, the server creates it when the volume is used for a specific IBM Spectrum Protect storage operation. The data set is not created when the volume is defined. Data loss can result when defining volumes because the z/OS media server reuses the volume or VSAM LDS if it exists at the time of allocation time. Important: To allow the server to generate volume names, consider using SCRATCH volumes.	AIX Linux SERVER1.BFS.POOL3.VOLA

Table 4. Volume name requirements for tape

Volume Name Requirements	Example
Use 1 - 32 alphanumeric characters. The volume name cannot contain any embedded blanks or equal signs.	DSMT01

AIX Linux

Table 5. z/OS media server: Volume name requirements for tape

Volume Name Requirements	Example
For tape cartridges, specify a tape volume name with 1 - 6 alphanumeric characters. The server converts tape volume names to uppercase. The volume name cannot contain any embedded blanks or equal signs. Each volume that is used by a server for any purpose must have a unique name. This requirement applies to all volumes, whether the volumes are used for storage pools, or used for operations such as database backup or export. The requirement also applies to volumes that reside in different z/OS media libraries but that are used by the same server.	DSMT01

Table 6. Volume name requirements for REMOVABLEFILE

Volume Name Requirements	Example

Volume Name Requirements	Example
1–6 alphanumeric characters The server converts volume names to uppercase.	`DSM01`

ACCess
Specifies how client nodes and server processes (such as migration) can access files in the storage pool volume. This parameter is optional. The default value is READWRITE. Possible values are:

READWrite
Specifies that client nodes and server processes can read from and write to files stored on the volume.
READOnly
Specifies that client nodes and server processes can only read files that are stored on the volume.
UNAVailable
Specifies that client nodes or server processes cannot access files that are stored on the volume.

If you define a random access volume as UNAVAILABLE, you cannot vary the volume online.

If you define a sequential access volume as UNAVAILABLE, the server does not attempt to access the volume.

OFfsite
Specifies that the volume is at an offsite location from which it cannot be mounted. You can specify this value only for volumes in copy or active-data storage pools.
Use this value to help you track volumes at offsite locations. The server treats volumes that are designated as offsite differently:

- The server does not generate mount requests for volumes designated offsite.
- The server reclaims or moves data from offsite volumes by retrieving files from other storage pools.
- The server does not automatically delete empty, offsite scratch volumes from a copy or active-data storage pool.

LOcation
Specifies the location of the volume. This parameter is optional. It can be specified only for volumes in sequential access storage pools. The location information can be a maximum length of 255 characters. Enclose the location in quotation marks if it contains any blank characters.
Formatsize
Specifies the size of the random access volume or FILE volume that is created and formatted in one step. The value is specified in megabytes. The maximum size is 8 000 000 MB (8 terabytes). This parameter is required if any of the following conditions are true:

- A single FILE or DISK volume is specified, which is to be created and formatted in one step.
- The value for the NUMBEROFVOLUMES parameter is greater than 1, and DISK volumes are being created.
- The value of the NUMBEROFVOLUMES parameter is greater than 1, and the value of the FORMATSIZE parameter is less than or equal to the MAXCAPACITY parameter of the DEFINE DEVCLASS command.

If you are allocating volumes on a z/OS media server, this parameter is not valid.

For a FILE volume, you must specify a value less than or equal to the value of the MAXCAPACITY parameter of the device class associated with the storage pool.

You cannot use this parameter for multiple, predefined volumes. Unless you specify `WAIT=YES` is specified, the operation is completed as a background process.

Numberofvolumes
Specifies the number of volumes that are created and formatted in one step. This parameter applies only to storage pools with DISK or FILE device classes. This parameter is optional. The default is 1. If you specify a value greater than 1, you must also specify a value for the FORMATSIZE parameter. Specify a number from 1 to 256.

If you are allocating volumes on a z/OS media server, the only value that this parameter supports is the default value of 1.

If the value for the NUMBEROFVOLUMES parameter is greater than 1, the volume name you specified will have a numeric suffix appended to create each name, for example, tivolivol001 and tivolivol002. Be sure to chose a volume name so that a valid file name for the target file system is created when the suffix is appended.

Important: You must ensure that storage agents can access newly created FILE volumes. For more information, see DEFINE PATH (Define a path).

Wait

Specifies whether volume creation and formatting operation is completed in the foreground or background. This parameter is optional. It is ignored unless you also specify the FORMATSIZE parameter.

No

Specifies that a volume creation and formatting operation is completed in the background. The NO value is the default when you also specify a format size.

Yes

Specifies that a volume creation and formatting operation is completed in the foreground.
Remember: You cannot specify `WAIT=YES` from the server console.

Example: Use a background process to define a new 100 MB volume for a disk storage pool

Create a volume of 100 MB in the disk storage pool named BACKUPPOOL. AIX Linux The volume name is /var/storage/bf.dsm. Windows The volume name is j:\storage\bf.dsm. Let the volume be created as a background process. AIX Linux

```
define volume backuppool
/var/storage/bf.dsm formatsize=100
```

Windows

```
define volume backuppool j:\storage\bf.dsm formatsize=100
```

Example: Define a volume to a disk storage pool with read and write access

A storage pool named POOL1 is assigned to a tape device class. Define a volume named TAPE01 to this storage pool, with READWRITE access.

```
define volume pool1 tape01 access=readwrite
```

Example: Define a volume to a file storage pool

A storage pool that is named FILEPOOL is assigned to a device class with a device type of FILE. AIX Linux Define a volume that is named filepool_vol01 to this storage pool. Windows Define a volume that is named fp_vol01.dsm to this storage pool. AIX Linux

```
define volume filepool /usr/storage/filepool_vol01
```

Windows

```
define volume filepool j:\storage\fp_vol01.dsm
```

Example: Example: Use a background process to define 10 volumes for a file storage pool with a device class 5 GB maximum capacity

Define 10 volumes in a sequential storage pool that uses a FILE device class. The storage pool is named FILEPOOL. The value of the MAXCAPACITY parameter for the device class that is associated with this storage pool is 5 GB. Creation must occur in the background.

```
define volume filepool filevol numberofvolumes=10 formatsize=5000
```

The server creates volume names filevol001 through filevol010.

Volumes are created in the directory or directories that are specified with the DIRECTORY parameter of the device class that is associated with storage pool filepool. If you specified multiple directories for the device class, individual volumes can be created in any of the directories in the list.

Related commands

Table 7. Commands related to DEFINE VOLUME

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.

Command	Description
QUERY VOLUME	Displays information about storage pool volumes.
UPDATE DEVCLASS	Changes the attributes of a device class.
UPDATE LIBVOLUME	Changes the status of a storage volume.
UPDATE VOLUME	Updates the attributes of storage pool volumes.

DELETE commands

Use the DELETE commands to delete or remove an IBM Spectrum Protect™ object.

- DELETE ASSOCIATION (Delete the node association to a schedule)
- DELETE ALERTTRIGGER (Remove a message from an alert trigger)
- DELETE BACKUPSET (Delete a backup set)
- DELETE CLIENTOPT (Delete an option in an option set)
- DELETE CLOPTSET (Delete a client option set)
- DELETE COLLOCGROUP (Delete a collocation group)
- DELETE COLLOCMEMBER (Delete collocation group member)
- DELETE COPYGROUP (Delete a backup or archive copy group)
- DELETE DATAMOVER (Delete a data mover)
- DELETE DEDUPSTATS (Delete data deduplication statistics)
- DELETE DEVCLASS (Delete a device class)
- DELETE DOMAIN (Delete a policy domain)
- DELETE DRIVE (Delete a drive from a library)
- DELETE EVENT (Delete event records)
- DELETE EVENTSERVER (Delete the definition of the event server)
- DELETE FILESPACE (Delete client node data from the server)
- DELETE GRPMEMBER (Delete a server from a server group)
- DELETE LIBRARY (Delete a library)
- DELETE MACHINE (Delete machine information)
- DELETE MACHNODEASSOCIATION (Delete association between a machine and a node)
- DELETE MGMTCLASS (Delete a management class)
- DELETE NODEGROUP (Delete a node group)
- DELETE NODEGROUPMEMBER (Delete node group member)
- DELETE PATH (Delete a path)
- DELETE POLICYSET (Delete a policy set)
- DELETE PROFASSOCIATION (Delete a profile association)
- DELETE PROFILE (Delete a profile)
- DELETE RECMEDMACHASSOCIATION (Delete recovery media and machine association)
- DELETE RECOVERYMEDIA (Delete recovery media)
- DELETE SCHEDULE (Delete a client or an administrative command schedule)
- DELETE SCRIPT (Delete command lines from a script or delete the entire script)
- DELETE SERVER (Delete a server definition)
- DELETE SERVERGROUP (Delete a server group)
- DELETE SPACETRIGGER (Delete the storage pool space triggers)
- DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)
- DELETE STGRULE (Delete storage rules for storage pools)
- DELETE STGPOOL (Delete a storage pool)
- DELETE STGPOOLDIRECTORY (Deleting a storage pool directory)
- DELETE SUBSCRIBER (Delete subscriptions from a configuration manager database)
- DELETE SUBSCRIPTION (Delete a profile subscription)
- DELETE VIRTUALFSMAPPING (Delete a virtual file space mapping)
- DELETE VOLHISTORY (Delete sequential volume history information)
- DELETE VOLUME (Delete a storage pool volume)

DELETE ALERTTRIGGER (Remove a message from an alert trigger)

Use this command to remove a message from the list of alert triggers.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                        .-,-----------------.
                        V                   |
>>-DELete ALERTTrigger----+--message_number-+------------------><
```

Parameters

message_number (Required)
: Specifies the message number that you want to remove from the list of alert triggers. Specify multiple message numbers, which are separated by commas, and no intervening spaces. Message numbers are a maximum of eight characters in length. Wildcard characters can be used to specify message numbers.

Delete alert trigger

Delete two message numbers that are designated as alerts, by issuing the following command:

```
delete alerttrigger ANR1067E,ANR1073E
```

Related commands

Table 1. Commands related to DELETE ALERTTRIGGER

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

DELETE ASSOCIATION (Delete the node association to a schedule)

Use this command to delete the association of a client node to a client schedule. IBM Spectrum Protect™ no longer runs the schedule on the client node.

If you try to disassociate a client from a schedule to which it is not associated, this command has no effect for that client.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege
- Restricted policy privilege for the domain to which the schedule belongs

Syntax

```
>>-DELete ASSOCiation--domain_name--schedule_name--------------->

   .-,---------.
```

```
   V           |
>----node_name-+-----------------------------------------><
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the schedule belongs.

schedule_name (Required)
: Specifies the name of the schedule from which clients are to be disassociated.

node_name (Required)
: Specifies the name of the client node that is no longer associated with the client schedule. You can specify a list of clients which are to be no longer associated with the specified schedule. Commas, with no intervening spaces, separate the items in the list. You can also use a wildcard character to specify a name. All matching clients are disassociated from the specified schedule.

Example: Delete a node association to a schedule

To delete the association of the node JEFF, assigned to the DOMAIN1 policy domain, to the WEEKLY_BACKUP schedule issue the following command:

```
delete association domain1 weekly_backup jeff
```

Example: Delete a node association to a schedule using a wildcard for node selection

Delete the association of selected clients, assigned to the DOMAIN1 policy domain, to the WEEKLY_BACKUP schedule so that this schedule is no longer run by these clients. The nodes that are disassociated from the schedule contain ABC or XYZ in the node name. Issue the command:

```
delete association domain1 weekly_backup *abc*,*xyz*
```

Related commands

Table 1. Commands related to DELETE ASSOCIATION

Command	Description
DEFINE ASSOCIATION	Associates clients with a schedule.
QUERY ASSOCIATION	Displays the clients associated with one or more schedules.

DELETE BACKUPSET (Delete a backup set)

Use this command to manually delete a backup set before its retention period expires.

When the server creates a backup set, the retention period assigned to the backup set determines how long the backup set remains in the database. When that date passes, the server automatically deletes the backup set when expiration processing runs. However, you can also manually delete the client's backup set from the server before it is scheduled to expire by using the DELETE BACKUPSET command.

Attention: If the volumes contain multiple backup sets, they are not returned to scratch status until all the backup sets are expired or are deleted.

Privilege class

If the REQSYSAUTHOUTFILE server option is set to YES (the default), the administrator must have system privilege. If the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax

```
              .-,------------------.
              V                    |
```

```
>>-DELete BACKUPSET----+-node_name-------+-+-------------------->
                       '-node_group_name-'

   .-,---------------.
   V                 |
>----backup_set_name-+--+--------------------+------------------>
                         '-BEGINDate--=--date-'

>--+---------------------+--+------------------+----------------->
   '-BEGINTime--=--time-'   '-ENDDate--=--date-'

                           .-WHEREDATAType--=--ALL-----------.
>--+------------------+--+-----------------------------------+---->
   '-ENDTime--=--time-'  |                    .-,---------. |
                         |                   V           | |
                         '-WHEREDATAType--=-----+-FILE--+-+-'
                                                '-IMAGE-'

>--+--------------------------------+--------------------------->
   '-WHERERETention--=--+-days----+-'
                        '-NOLimit-'

>--+-----------------------------------+------------------------->
   '-WHEREDESCription--=--description-'

   .-Preview -=--No------.
>--+---------------------+-------------------------------------><
   '-Preview--=--+-No--+-'
                 '-Yes-'
```

Parameters

node_name or node_group_name (Required)

Specifies the name of the client nodes or node groups whose data is contained in the specified backup set volumes. To specify multiple node and node group names, separate the names with commas and no intervening spaces. Any node name you specify may contain wildcard characters, but node group names cannot contain wildcard characters. If backup set volumes contain backup sets from multiple nodes then every backup set whose node name matches one of the specified node names will be deleted.

backup_set_name (Required)

Specifies the name of the backup set to delete. The backup set name you specify can contain wildcard characters. You can specify more than one backup set name by separating the names with commas and no intervening spaces.

BEGINDate

Specifies the beginning date in which the backup set to delete was created. This parameter is optional. You can use this parameter with the BEGINTIME parameter to specify a range for the date and time. If you specify a begin date without a begin time, the time will be at 12:00 a.m. (midnight) on the date you specify.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified.	TODAY +3 *or* +3.
TODAY-days *or* -days	The current date minus days specified.	TODAY -3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time in which the backup set to delete was created. This parameter is optional. You can use this parameter in conjunction with the BEGINDATE parameter to specify a range for the date and time. If you specify a begin time without a begin date, the date will be the current date at the time you specify.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes specified	NOW+02:00 *or* +02:00.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes specified	NOW-02:00 *or* –02:00.

ENDDate

Specifies the ending date in which the backup set to delete was created. This parameter is optional. You can use this parameter in conjunction with the ENDTIME parameter to specify a range for the date and time. If you specify an end date without an end time, the time will be at 11:59:59 p.m. on the specified end date.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified.	TODAY +3 *or* +3.
TODAY-days *or* -days	The current date minus days specified.	TODAY -3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time of the range in which the backup set to delete was created. This parameter is optional. You can use this parameter in conjunction with the ENDDATE parameter to specify a range for the date and time. If you specify an end time without an end date, the date will be the current date at the time you specify.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date	NOW+02:00 *or* +02:00.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date	NOW-02:00 *or* -02:00.

WHEREDATAType

Specifies the backup sets containing the specified types of data are to be deleted. This parameter is optional. The default is that backup sets for all types of data (file level, image, and application) are to be deleted. To specify multiple data types, separate the data types with commas and no intervening spaces. Possible values are:

ALL
: Specifies that backup sets for all types of data (file level, image, and application) are to be deleted. This is the default.

FILE
: Specifies that a file level backup set is to be deleted. File level backup sets contain files and directories backup up by the backup-archive client.

IMAGE
: Specifies that an image backup set is to be deleted. Image backup sets contain images created by the backup-archive client BACKUP IMAGE command.

WHERERETention
: Specifies the retention value, specified in days, that is associated with the backup sets to delete. You can specify an integer from 0 to 30000. The values are:

days
: Specifies that backup sets that are retained this number of days are deleted.

NOLimit
: Specifies that the backup sets that are retained indefinitely are deleted.

WHEREDESCription
: Specifies the description that is associated with the backup set to delete. The description you specify can contain a wildcard character. This parameter is optional. Enclose the description in quotation marks if it contains any blank characters.

Preview
: Specifies whether to preview the list of backup sets to delete, without actually deleting the backup sets. This parameter is optional. The default value is NO. The values are:

No
: Specifies that the backup sets are deleted.

Yes
: Specifies that the server displays the list of backup sets to delete, without actually deleting the backup sets.

Example: Delete a backup set

Delete backup set named PERS_DATA.3099 that belongs to client node JANE. The backup set was generated on 11/19/1998 at 10:30:05 and the description is "Documentation Shop".

```
delete backupset pers_data.3099
begindate=11/19/1998 begintime=10:30:05
wheredescription="documentation shop"
```

Related commands

Table 1. Commands related to DELETE BACKUPSET

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.

Command	Description
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

DELETE CLIENTOPT (Delete an option in an option set)

Use this command to delete a client option in an option set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege.

Syntax

```
>>-DELete CLIENTOpt--option_set_name--option_name--------------->

>--+-------------------------+------------------------------><
   '-SEQnumber--=--+-number-+-'
                   '-ALL----'
```

Parameters

option_set_name (Required)
: Specifies the name of the client option set.

option_name (Required)
: Specifies a valid client option.

SEQnumber
: Specifies a sequence number when an option name is specified more than once. This parameter is optional. Valid values are:

  n
  : Specifies an integer of 0 or greater.

  ALL
  : Specifies all sequence numbers.

Example: Delete the date format option

Delete the date format option in an option set named *ENG*.

```
delete clientopt eng dateformat
```

Related commands

Table 1. Commands related to DELETE CLIENTOPT

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLOPTSET	Deletes a client option set.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.

DELETE CLOPTSET (Delete a client option set)

Use this command to delete a client option set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege.

Syntax

```
>>-DELete CLOptset--option_set_name---------------------------><
```

Parameters

option_set_name (Required)
Specifies the name of the client option set to delete.

Example: Delete a client option set

Delete the client option set named ENG.

```
delete cloptset eng
```

Related commands

Table 1. Commands related to DELETE CLOPTSET

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.

DELETE COLLOCGROUP (Delete a collocation group)

Use this command to delete a collocation group. You cannot delete a collocation group if it has any members in it.

You can remove all the members in the collocation group by issuing the DELETE COLLOCMEMBER command with a wildcard in the node_name parameter.

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

```
>>-DELete COLLOCGroup--group_name-----------------------------><
```

Parameters

group_name
Specifies the name of the collocation group that you want to delete.

Example: Delete a collocation group

Delete a collocation group named group1.

```
delete collocgroup group1
```

Related commands

Table 1. Commands related to DELETE COLLOCGROUP

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

DELETE COLLOCMEMBER (Delete collocation group member)

Use this command to delete a client node or file space from a collocation group.

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

```
Delete a node from a collocation group

                                    .-,---------.
                                    V           |
>>-DELete COLLOCMember--group_name----node_name-+--------------><
```

Parameters

group_name
Specifies the name of the collocation group from which you want to delete a client node.
node_name

Specifies the name of the client node that you want to delete from the collocation group. You can specify one or more names. When you specify multiple names, separate the names with commas; do not use intervening spaces. You can also use wildcard characters to specify multiple nodes.

```
Delete a file space from a file space collocation group

>>-DELete COLLOCMember--group_name--node_name------------------->

                 .-,---------------.
                 V                 |
>--FIlespace--=----file_space_name-+--------------------------->

   .-NAMEType--=--SERVER------.
>--+--------------------------+-------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+----------------------------><
   '-CODEType--=--+-BOTH-------+-'
                  +-UNIcode----+
                  '-NONUNIcode-'
```

Parameters

group_name
: Specifies the name of the collocation group from which you want to delete a file space.

node_name
: Specifies the client node where the file space is located.

FIlespace
: Specifies the *file_space_name* on the client node that you want to delete from the collocation group. You can specify one or more file space names that are on a specific client node. If you specify multiple file space names, separate the names with commas, and do not use intervening spaces. You can also use wildcard characters when you specify multiple file space names.

NAMEType
: Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with Unicode support. A backup-archive client with Unicode support is available only for Windows, Macintosh OS 9, Macintosh OS X, and NetWare. Use this parameter when you specify a file space name that is not a single wildcard. You can specify a fully qualified file space name, which does not have a wildcard. Or you can specify a partly qualified file space name, which can have a wildcard but must contain other characters. The default value is SERVER. Possible values are

  SERVER
  : The server uses the server code page to interpret the file space names.

  UNIcode
  : The server converts the file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the names and the server code page. Conversion might fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

  FSID
  : The server interprets the file space names by their file space IDs (FSIDs).

CODEType
: Specify how you want the server to interpret the file space names that you enter. Use this parameter only when you use a single wildcard character for the file space name. The default is BOTH, so the file spaces are included, regardless of code page type. The following values are available:

  BOTH
  : Include the file spaces, regardless of code page type.

  UNIcode
  : Include file spaces that are in Unicode only.

NONUNIcode
Include file spaces that are not in Unicode.

Delete collocation group members

Delete two nodes, NODE1 and NODE2, from a collocation group, GROUP1.

```
delete collocmember group1 node1,node2
```

Delete a file space from a file space collocation group

Issue the following command to delete files space *cap_27400* from collocation group *collgrp_2* on node *hp_4483*:

```
delete collocmember collgrp_2 hp_4483 filespace=cap_27400
```

Delete a file space collocation group member from a node that uses Unicode

If the file space is on a node that uses Unicode, you can specify that in the command. Issue the following command to delete file space *cap_257* from collocation group *collgrp_3* from the *win_4687* node:

```
delete collocmember collgrp_3 win_4687 filespace=cap_257 codetype=unicode
```

Delete a file space with a partial name designated

If the file space has a partial name, you can use a wildcard to delete it. Issue the following command to delete file space *cap_* from collocation group *collgrp_4* from *win_4687* node:

```
delete collocmember collgrp_4 win_4687 filespace=cap_* codetype=unicode
```

If there is more than one file space whose name begins with cap_, those file spaces are also deleted.

Related commands

Table 1. Commands related to DELETE COLLOCMEMBER

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

DELETE COPYGROUP (Delete a backup or archive copy group)

Use this command to delete a backup or archive copy group from a management class. You cannot delete a copy group in the ACTIVE policy set.

When you activate the changed policy set, any files that are bound to a deleted copy group are managed by the default management class.

You can delete the predefined STANDARD copy group in the STANDARD policy domain (STANDARD policy set, STANDARD management class). However, if you later reinstall the IBM Spectrum Protect™ server, the process restores all STANDARD policy objects.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the copy group belongs.

Syntax

```
>>-DELete COpygroup--domain_name--policy_set_name--class_name--->

   .-STANDARD-.  .-Type--=--Backup------.
>--+----------+--+---------------------+---------------------><
   '-STANDARD-'  '-Type--=--+-Backup--+-'
                            '-Archive-'
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the copy group belongs.

policy_set_name (Required)
: Specifies the policy set to which the copy group belongs.

class_name (Required)
: Specifies the management class to which the copy group belongs.

STANDARD
: Specifies the copy group, which is always STANDARD. This parameter is optional. The default value is STANDARD.

Type
: Specifies the type of copy group to delete. This parameter is optional. The default value is BACKUP. Possible values are:

  Backup
  : Specifies that the backup copy group is deleted.

  Archive
  : Specifies that the archive copy group is deleted.

Example: Delete a backup copy group

Delete the backup copy group from the ACTIVEFILES management class that is in the VACATION policy set of the EMPLOYEE_RECORDS policy domain.

```
delete copygroup employee_records
vacation activefiles
```

Example: Delete an archive copy group

Delete the archive copy group from the MCLASS1 management class that is in the SUMMER policy set of the PROG1 policy domain.

```
delete copygroup prog1 summer mclass1 type=archive
```

Related commands

Table 1. Commands related to DELETE COPYGROUP

Command	Description
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
QUERY COPYGROUP	Displays the attributes of a copy group.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

DELETE DATAMOVER (Delete a data mover)

Use this command to delete a data mover. You cannot delete the data mover if any paths are defined for this data mover.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DELete DATAMover--data_mover_name--------------------------><
```

Parameters

data_mover_name (Required)
Specifies the name of the data mover.
Note: This command deletes the data mover even if there is data for the corresponding NAS node.

Example: Delete a data mover

Delete the data mover for the node named NAS1.

```
delete datamover nas1
```

Related commands

Table 1. Commands related to DELETE DATAMOVER

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE PATH	Defines a path from a source to a destination.
DELETE PATH	Deletes a path from a source to a destination.
QUERY DATAMOVER	Displays data mover definitions.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DATAMOVER	Changes the definition for a data mover.

AIX Linux Windows

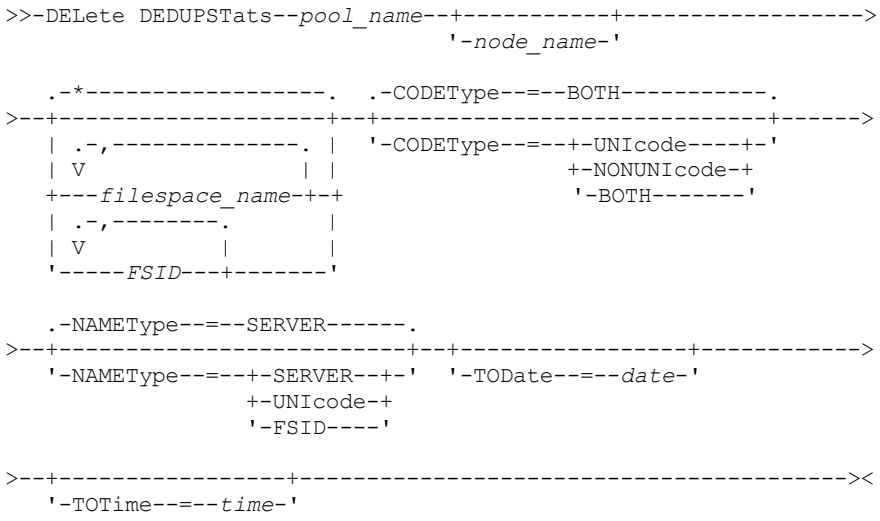
DELETE DEDUPSTATS (Delete data deduplication statistics)

Use this command to delete data deduplication statistics for a directory-container storage pool or a cloud storage pool. You cannot delete the most recent data deduplication statistics for a client node and a file space.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool.

Syntax



Parameters

pool_name (Required)
: Specifies the name of the directory-container storage pool that is reported in the data deduplication statistics. You can specify up to 30 characters for the storage pool name. If you specify more than 30 characters the command fails.
Restriction: You can only specify directory-container storage pools or cloud storage pools.

node_name
: Specifies the name of the client node that is reported in the data deduplication statistics. This parameter is optional. If you do not specify a value for this parameter, all nodes are displayed. You can specify up to 64 characters for the node name. If you specify more than 64 characters the command fails.

filespace_name or FSID
: Specifies the name or file space ID (FSID) of one or more file spaces that is reported in the data deduplication statistics. This parameter is optional. You can use wildcard characters to specify this name. An asterisk is the default. Specify one of the following values:

  *
  : Specify an asterisk (*) to show all file spaces or IDs.

  filespace_name
  : Specifies the name of the file space. Specify more than one file space by separating the names with commas and no intervening spaces. FSID Specifies the file space identifier. This parameter is valid for clients with file spaces that are in Unicode format. Specify more than one file space by separating the names with commas and no intervening spaces.

  For clients with file spaces that are in Unicode format, you can enter either a file space name or a FSID. If you enter a file space name, the server might have to convert the file space name that you enter. For example, the server might have to convert the name that you enter from the server's code page to Unicode.
  Restrictions: The following restrictions apply to file space names and file space identifiers (FSID):

  - You must specify a node name if you specify a file space name.
  - Do not specify both file space names and FSIDs on the same command.

CODEType
: Specifies what type of file spaces to include in the report. The default value is BOTH, which specifies that file spaces are included regardless of code page type. Use this parameter only when you enter an asterisk to display information about all file spaces. This parameter is optional. Specify one of the following values:

  UNIcode
  : Include file spaces that are in Unicode format.

  NONUNIcode
  : Include file spaces that are not in Unicode format.

  BOTH

Include file spaces regardless of code page type. This is the default.

NAMEType

Specifies how you want the server to interpret the file space names that you enter. Use this parameter when IBM Spectrum Protect™ clients have file spaces that are in Unicode format, and are on Windows, NetWare, or Macintosh OS X operating systems. This parameter is optional.
This parameter is required if you specify a node name and a file space name or FSID.
Restriction: When you specify this parameter, the file space name cannot contain an asterisk.

Specify one of the following values:

SERVER
: The server uses the server's code page to interpret the file space names. This is the default.

UNIcode
: The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

FSID
: The server interprets the file space names as their file space IDs (FSIDs).

TODate

Specifies the latest date for statistics to be deleted. IBM Spectrum Protect deletes only those statistics with a date on or before the date you specify. This parameter is optional.
Specify one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date.	10/15/2015 If you specify a date, all candidate records that are written on that day (ending at 11:59:59 pm) will be evaluated.
TODAY	The current date.	TODAY
TODAY-days or -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 or –1. To display information that is created until yesterday, you can specify TODATE=TODAY-1 or TODATE= -1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include records that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include records that were active on the 10th day of the current month.

TOTime

Specifies that you want to delete data deduplication statistics that are created on or before this time on the specified date. This parameter is optional. The default is the end of the day (23:59:59). Specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified date.	12:30:22
NOW	The current time on the specified date.	NOW

Value	Description	Example
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified date.	NOW+03:00 or +03:00. If you issue the DELETE DEDUPSTATS command at 9:00 with TOTIME=NOW+03:00 or TOTIME=+03:00, IBM Spectrum Protect deletes records with a time of 12:00 or earlier on the specified date.
NOW-HH:MM or -HH:MM	The current time minus hours and minutes on the specified date.	NOW-03:30 or -03:30. If you issue the DELETE DEDUPSTATS command at 9:00 with TOTIME=NOW-3:30 or TOTIME=-3:30, IBM Spectrum Protect deletes records with a time of 5:30 or earlier on the specified date.

Example: Delete data deduplication statistics for a file space

Delete data deduplication statistics of a file space that is called /srvr that belongs to a directory-container storage pool, POOL1, that is stored on client node NODE1.

```
delete dedupstats pool1 node1 /srvr
```

Related commands

Table 1. Commands related to DELETE DEDUPSTATS

Command	Description
GENERATE DEDUPSTATS	Generates data deduplication statistics.
AIX Linux Windows QUERY DEDUPSTATS	Displays data deduplication statistics.

DELETE DEVCLASS (Delete a device class)

Use this command to delete a device class.

To use this command, you must first delete all storage pools that are assigned to the device class and, if necessary, cancel any database export or import processes that are using the device class.

You cannot delete the device class DISK, which is predefined at installation, but you can delete any device classes defined by the IBM Spectrum Protect™ administrator.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DELete DEVclass--device_class_name-------------------------><
```

Parameters

device_class_name (Required)
Specifies the name of the device class to be deleted.

Example: Delete a device class

Delete the device class named MYTAPE. There are no storage pools assigned to the device class.

```
delete devclass mytape
```

Related commands

Table 1. Commands related to DELETE DEVCLASS

Command	Description
DEFINE DEVCLASS	Defines a device class.
AIX Linux DEFINE DEVCLASS (z/OS® media server)	AIX Linux Defines a device class to use storage managed by a z/OS media server.
QUERY DEVCLASS	Displays information about device classes.
QUERY DIRSPACE	Displays information about FILE directories.
UPDATE DEVCLASS	Changes the attributes of a device class.
AIX Linux UPDATE DEVCLASS (z/OS media server)	AIX Linux Changes the attributes of a device class for storage managed by a z/OS media server.

DELETE DOMAIN (Delete a policy domain)

Use this command to delete a policy domain. All associated policy sets, including the ACTIVE policy set, management classes, and copy groups are deleted along with the policy domain.

You cannot delete a policy domain to which client nodes are registered. To determine if any client nodes are registered to a policy domain, issue the QUERY DOMAIN or the QUERY NODE command. Move any client nodes to another policy domain, or delete the nodes.

You can delete the predefined STANDARD policy domain. However, if you later reinstall the IBM Spectrum Protect™ server, the process restores all STANDARD policy objects.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete DOmain--domain_name---------------------------------><
```

Parameters

domain_name (Required)
Specifies the policy domain to delete.

Examples: Delete a policy domain

Delete the EMPLOYEE_RECORDS policy domain.

```
delete domain employee_records
```

Related commands

Table 1. Commands related to DELETE DOMAIN

Command	Description
COPY DOMAIN	Creates a copy of a policy domain.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
QUERY DOMAIN	Displays information about policy domains.
UPDATE DOMAIN	Changes the attributes of a policy domain.

DELETE DRIVE (Delete a drive from a library)

Use this command to delete a drive from a library. A drive that is in use cannot be deleted.

All paths related to a drive must be deleted before the drive itself can be deleted.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DELete DRive--library_name--drive_name---------------------><
```

Parameters

library_name (Required)
: Specifies the name of the library where the drive is located.

drive_name (Required)
: Specifies the name of the drive to be deleted.

Example: Delete a drive from a library

Delete DRIVE3 from the library named AUTO.

```
delete drive auto drive3
```

Related commands

Table 1. Commands related to DELETE DRIVE

Command	Description
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE LIBRARY	Deletes a library.
DELETE PATH	Deletes a path from a source to a destination.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
UPDATE DRIVE	Changes the attributes of a drive.

DELETE EVENT (Delete event records)

Use this command to delete event records from the database. An event record is created whenever processing of a scheduled command is started or missed.

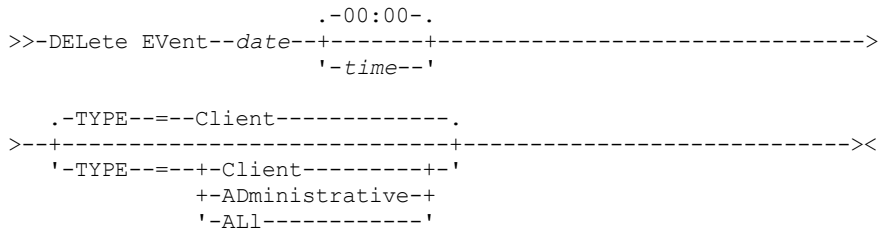
This command only deletes the event records that exist at the time the command is processed. An event record will not be found:

- If the event record has never been created (the event is scheduled for the future)
- If the event has passed and the event record has already been deleted.

Privilege class

To issue this command, you must have system privilege or unrestricted policy privilege.

Syntax



Parameters

date (Required)

Specifies the date used to determine which event records to delete. The maximum number of days you can specify is 9999.

Use this parameter in conjunction with the TIME parameter to specify a date and time for deleting event records. Any record whose scheduled start occurs before the specified date and time is deleted. However, records are not deleted for events whose startup window has not yet passed.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified	TODAY-3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

time

Specifies the time used to determine which event records to delete. Use this parameter in conjunction with the DATE parameter to specify a date and time for deleting event records. Any record whose scheduled start occurs before the specified date and time is deleted. However, records are not deleted for events whose startup window has not yet passed. The default is 00:00.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes specified	NOW+03:00 or +03:00 Attention: If you issue this command at 9:00 using NOW+03:00 *or* +03:00, IBM Spectrum Protect™ deletes records with a time of 12:00 or later on the date you specify.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes specified	NOW-03:00 *or* –03:00

TYPE

Specifies the type of events to be deleted. This parameter is optional. The default is CLIENT. Possible values are:

Client
: Specifies to delete event records for client schedules.

ADministrative
: Specifies to delete event records for administrative command schedules.

ALl
: Specifies to delete event records for both client and administrative command schedules.

Example: Delete event records

Delete records for events with scheduled start times prior to 08:00 on May 26, 1998 (05/26/1998), and whose startup window has passed. Records for these events are deleted regardless of whether the retention period for event records, as specified with the SET EVENTRETENTION command, has passed.

```
delete event 05/26/1998 08:00
```

Related commands

Table 1. Commands related to DELETE EVENT

Command	Description
QUERY EVENT	Displays information about scheduled and completed events for selected clients.
SET EVENTRETENTION	Specifies the number of days to retain records for scheduled operations.

DELETE EVENTSERVER (Delete the definition of the event server)

Use this command to delete the definition of the event server. You must issue this command before you issue the DELETE SERVER command. If you specify the server defined as the event server on the DELETE SERVER command, you will receive an error message.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete EVENTSERVer-----------------------------------------><
```

Example: Delete an event server definition

Delete the definition for the event server ASTRO.

```
delete eventserver
```

Related commands

Table 1. Commands related to DELETE EVENTSERVER

Command	Description
DEFINE EVENTSERVER	Defines a server as an event server.
QUERY EVENTSERVER	Displays the name of the event server.

DELETE FILESPACE (Delete client node data from the server)

Use this command to delete file spaces from the server. Files that belong to the file space are deleted from primary, active-data, and copy storage pools, and any file space collocation groups.

IBM Spectrum Protect™ deletes one or more file spaces as a series of batch database transactions, thus preventing a rollback or commit for an entire file space as a single action. If the process is canceled or if a system failure occurs, a partial deletion can occur. A subsequent DELETE FILESPACE command for the same node or owner can delete the remaining data.

If this command is applied to a WORM (write once, read many) volume, the volume is returned to scratch if it has space on which data can be written. (Data on WORM volumes, including deleted and expired data, cannot be overwritten. Therefore, data can be written only in space that does not contain current, deleted, or expired data.) If a WORM volume does not have any space available on which data can be written, it remains private. To remove the volume from the library, you must use the CHECKOUT LIBVOLUME command.

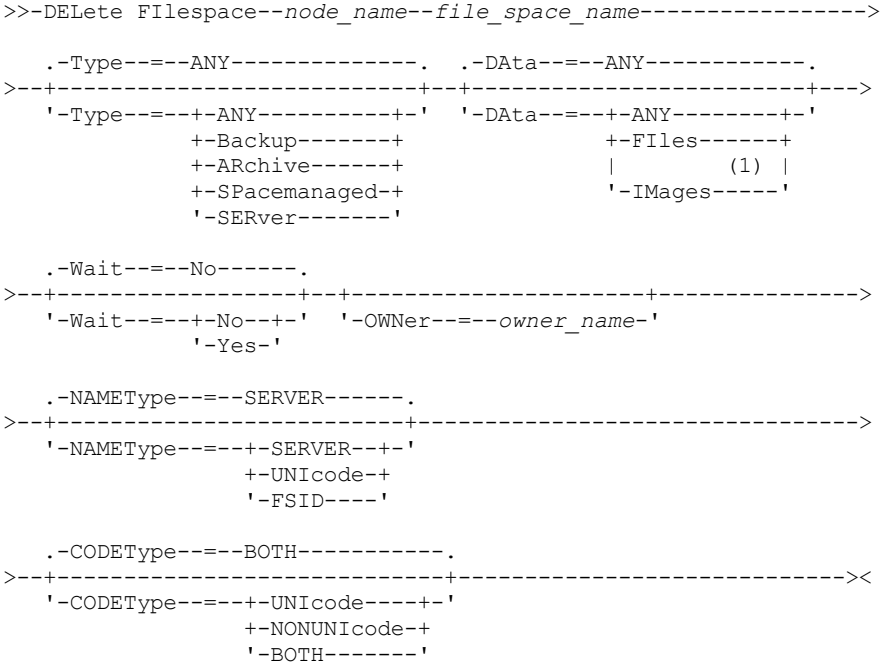
Tips:

- If archive retention protection is enabled, the server deletes archive files with expired retention periods. For more information, see the SET ARCHIVERETENTIONPROTECTION command.
- The server does not delete archive files that are on deletion hold until the hold is released.
- Reclamation does not start while the DELETE FILESPACE command is running.
- If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
- If you delete a file space in a deduplicated storage pool, the file space name DELETED is displayed in the output of the QUERY OCCUPANCY command until all deduplication dependencies are removed.
- When replication is configured for a file space, the DELETE FILESPACE command deletes only the file space on the server where you issued the command. If you issue the REPLICATE NODE command, the file space is not deleted on the other replication server.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax



Notes:

1. This parameter can be used only when `TYPE=ANY` or `TYPE=BACKUP` is specified.

Parameters

node_name (Required)

Specifies the name of the client node to which the file space belongs.

file_space_name (Required)

Specifies the name of the file space to be deleted. This name is case-sensitive and must be entered exactly as it is known to the server. To determine how to enter the name, use the QUERY FILESPACE command. You can use wildcard characters to specify this name.

For a server that has clients with support for Unicode, you might have the server convert the file space name that you enter. For example, you might want to have the server convert the name that you entered from the server's code page, to Unicode. See the NAMETYPE parameter for details. If you do not specify a file space name, or specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

Type

Specifies the type of data to be deleted. This parameter is optional. The default value is ANY. You can use the following values:

ANY

Delete only backed-up versions of files and archived copies of files.

If you specify `delete filespace node_name * type=any`, all backed-up data and archived data in all file spaces for that node are deleted. File spaces are deleted only if they do not contain files that are moved from an IBM Spectrum Protect for Space Management client.

Backup

Delete backup data for the file space.

ARchive

Delete all archived data on the server for the file space.

SPacemanaged

Delete files that are migrated from a user's local file system by an IBM Spectrum Protect for Space Management client. The OWNER parameter is ignored when you specify TYPE=SPACEMANAGED.

SERver

Delete all archived files in all file spaces for a node that is registered as TYPE=SERVER.

DAta

Specifies objects to delete. This parameter is optional. The default value is ANY. You can specify one of the following values:

ANY

Delete files, directories, and images.

FIles

Delete files and directories.

IMages

Delete image objects. You can use this parameter only if you specified TYPE=ANY or TYPE=BACKUP.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is No. You can specify one of the following values:

No

Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

Yes

Specifies that the server processes this command in the foreground. Wait for the command to complete before you continue with other tasks. The server displays the output messages to the administrative client when the command completes.
Restriction: You cannot specify WAIT=YES from the server console.

OWNer

Restricts the data that is deleted to files that belong to the owner. This parameter is optional; it is ignored when TYPE=SPACEMANAGED. This parameter applies to only multiuser client systems such as AIX®, Linux, and Solaris OS.

NAMEType

Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for Unicode. A backup-archive client with support for Unicode is available only for the following operating systems: Windows, Macintosh OS X, and NetWare operating systems.

Use this parameter only when you enter a partly or fully qualified file space name. The default value is SERVER. You can specify one of the following values:

SERVER
: The server uses the server's code page to interpret the file space names.

UNIcode
: The server converts the file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines.

FSID
: The server interprets the file space names as their file space IDs (FSIDs).

CODEType
: Specify what type of file spaces are to be included in the operation. The default is BOTH, meaning that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name. You can specify one of the following values:

UNIcode
: Include file spaces that are in Unicode.

NONUNIcode
: Include file spaces that are not in Unicode.

BOTH
: Include file spaces regardless of code page type.

Delete a file space

Delete the C_Drive file space that belongs to the client node HTANG.

```
delete filespace htang C_Drive
```

Delete all space-managed files for a client node

Delete all files that are migrated from client node APOLLO (that is, all space-managed files).

```
delete filespace apollo * type=spacemanaged
```

Related commands

Table 1. Commands related to DELETE FILESPACE

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY OCCUPANCY	Displays file space information by storage pool.
QUERY PROCESS	Displays information about background processes.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
RENAME FILESPACE	Renames a client filespace on the server.

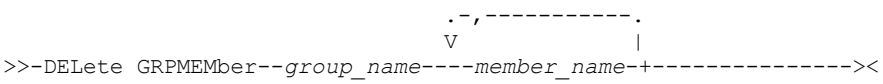
DELETE GRPMEMBER (Delete a server from a server group)

Use this command to delete a server or server group from a server group.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

group_name (Required)
: Specifies the group.

member_name (Required)
: Specifies the server or group to delete from the group. To specify multiple names, separate the names with commas and no intervening spaces.

Example: Delete a server from a server group

Delete member PHOENIX from group WEST_COMPLEX.

```
delete grpmember west_complex phoenix
```

Related commands

Table 1. Commands related to DELETE GRPMEMBER

Command	Description
DEFINE GRPMEMBER	Defines a server as a member of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE SERVER	Deletes the definition of a server.
DELETE SERVERGROUP	Deletes a server group.
MOVE GRPMEMBER	Moves a server group member.
QUERY SERVER	Displays information about servers.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

DELETE LIBRARY (Delete a library)

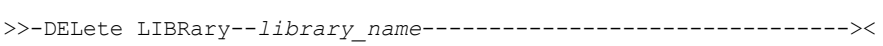
Use this command to delete a library. Before you delete a library, you must delete other associated objects, such as the path.

Use this command to delete a library. Before you delete a library, delete the path and all associated drives.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

library_name (Required)
Specifies the name of the library to be deleted.

Example: Delete a manual library

Delete the manual library named LIBR1.

```
delete library libr1
```

Related commands

Table 1. Commands related to DELETE LIBRARY

Command	Description
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DRIVE	Deletes a drive from a library.
DELETE PATH	Deletes a path from a source to a destination.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE LIBRARY	Changes the attributes of a library.
UPDATE PATH	Changes the attributes associated with a path.

DELETE MACHINE (Delete machine information)

Use this command to delete machine description information. To replace existing information, issue this command and then issue an INSERT MACHINE command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete MACHine--machine_name---------------------------------->

   .-Type--=--All----------------------.
>--+-----------------------------------+----------------------><
   '-Type--=--+-All------------------+-'
              +-RECOVERYInstructions-+
              '-CHaracteristics------'
```

Parameters

machine_name (Required)
Specifies the name of the machine whose information is to be deleted.

Type
Specifies the type of machine information. This parameter is optional. The default is ALL. Possible values are:

All

Specifies all information.

RECOVERYInstructions
: Specifies the recovery instructions.

CHaracteristics
: Specifies the machine characteristics.

Example: Delete a specific machine's information

Delete the machine characteristics associated with the DISTRICT5 machine.

```
delete machine district5 type=characteristics
```

Related commands

Table 1. Commands related to DELETE MACHINE

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
INSERT MACHINE	Inserts machine characteristics or recovery instructions into the IBM Spectrum ProtectIBM Spectrum Protect™ database.
QUERY MACHINE	Displays information about machines.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.
UPDATE MACHINE	Changes the information for a machine.

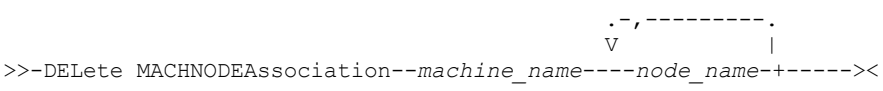
DELETE MACHNODEASSOCIATION (Delete association between a machine and a node)

Use this command to delete the association between a machine and one or more nodes. This command does not delete the node from IBM Spectrum Protect™.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

machine_name (Required)
: Specifies the name of a machine that is associated with one or more nodes.

node_name (Required)
: Specifies the name of a node associated with a machine. If you specify a list of node names, separate the names with commas and no intervening spaces. You can use wildcard characters to specify a name. If a node is not associated with the machine, that node is ignored.

Example: Delete an association between a node and a machine

Delete the association between the DISTRICT5 machine and the ACCOUNTSPAYABLE node.

```
delete machnodeassociation district5 accountspayable
```

Related commands

Table 1. Commands related to DELETE MACHNODEASSOCIATION

Command	Description
DEFINE MACHNODEASSOCIATION	Associates an IBM Spectrum Protect node with a machine.
QUERY MACHINE	Displays information about machines.

DELETE MGMTCLASS (Delete a management class)

Use this command to delete a management class. You cannot delete a management class in the ACTIVE policy set. All copy groups in the management class are deleted along with the management class.

You can delete the management class assigned as the default for a policy set, but a policy set cannot be activated unless it has a default management class.

You can delete the predefined STANDARD management class in the STANDARD policy domain. However, if you later reinstall the IBM Spectrum Protect™ server, the process restores all STANDARD policy objects.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the management class belongs.

Syntax

```
>>-DELete MGmtclass--domain_name--policy_set_name--class_name--><
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the management class belongs.

policy_set_name (Required)
: Specifies the policy set to which the management class belongs.

class_name (Required)
: Specifies the management class to delete.

Example: Delete a management class

Delete the ACTIVEFILES management class from the VACATION policy set of the EMPLOYEE_RECORDS policy domain.

```
delete mgmtclass employee_records
vacation activefiles
```

Related commands

Table 1. Commands related to DELETE MGMTCLASS

Command	Description
ASSIGN DEFMGMTCLASS	Assigns a management class as the default for a specified policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE MGMTCLASS	Defines a management class.
QUERY MGMTCLASS	Displays information about management classes.
UPDATE MGMTCLASS	Changes the attributes of a management class.

DELETE NODEGROUP (Delete a node group)

Use this command to delete a node group. You cannot delete a node group if it has any members in it.

Attention: You can remove all the members in the node group by issuing the DELETE NODEGROUPMEMBER command with a wildcard in the node_name parameter.

Privilege class

To issue this command, you must have system or unrestricted policy privilege.

Syntax

```
>>-DELete NODEGroup--group_name--------------------------------><
```

Parameters

group_name
: Specifies the name of the node group that you want to delete.

Example: Delete a node group

Delete a node group named `group1`.

```
delete nodegroup group1
```

Related commands

Table 1. Commands related to DELETE NODEGROUP

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

DELETE NODEGROUPMEMBER (Delete node group member)

Use this command to delete a client node from a node group.

Privilege class

To issue this command, you must have system or unrestricted policy privilege.

Syntax

```
                                    .-,---------.
                                    V           |
>>-DELete NODEGROUPMember--group_name----node_name-+-----------><
```

Parameters

group_name
: Specifies the name of the node group from which you want to delete a client node.

node_name
: Specifies the name of the client node that you want to delete from the node group. You can specify one or more names. When specifying multiple names, separate the names with commas; do not use intervening spaces. You can also use wildcard characters to specify multiple nodes.

Example: Delete node group members

Delete two nodes, `node1` and `node2`, from a node group, `group1`.

```
delete nodegroupmember group1 node1,node2
```

Related commands

Table 1. Commands related to DELETE NODEGROUPMEMBER

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

DELETE PATH (Delete a path)

Use this command to delete a path definition

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DELete PATH--source_name--destination_name------------------>

                          (1)
>--SRCType--=--+-DATAMover-----+-------------------------------->
               '-SERVer--------'

                        (2)
>--DESTType--=--+-DRive------LIBRary--=--library_name-+-------><
                '-LIBRary-----------------------------'
```

Notes:

1. This parameter is only available on AIX, HP-UX, Linux, Solaris, Windows operating systems.
2. This parameter is only available on AIX, HP-UX, Linux, Solaris, Windows operating systems.

Parameters

source_name (Required)
Specifies the name of the source of the path to be deleted. This parameter is required.

The name specified must be that of a server or data mover that is already defined to the server.

destination_name (Required)
Specifies the name of the destination of the path to be deleted. This parameter is required.

SRCType (Required)
Specifies the source type of the path to be deleted. This parameter is required. Possible values are:

DATAMover
Specifies that a data mover is the source.

SERVer
Specifies that a storage agent is the source.

DESTType (Required)
Specifies the type of the destination. Possible values are:

DRive LIBRary=library_name
Specifies that a drive is the destination. The DRIVE and LIBRARY parameters are both required when the destination type is drive.

LIBRary
Specifies that a library is the destination.
Attention: If the path from a data mover to a library is deleted, or the path from the server to a library is deleted, the server will not be able to access the library. If the server is halted and restarted while in this state, the library will not be initialized.

Example: Delete a NAS data mover path

Delete a path from a NAS data mover NAS1 to the library NASLIB.

```
delete path nas1 naslib srctype=datamover desttype=library
```

Related commands

Table 1. Commands related to DELETE PATH

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE PATH	Defines a path from a source to a destination.
PERFORM LIBACTION	Defines all drives and paths for a library.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE PATH	Changes the attributes associated with a path.

DELETE POLICYSET (Delete a policy set)

Use this command to delete a policy set. When you delete a policy set, all management classes and copy groups that belong to the policy set are also deleted.

The ACTIVE policy set in a policy domain cannot be deleted. You can replace the contents of the ACTIVE policy set by activating a different policy set. Otherwise, the only way to remove the ACTIVE policy set is to delete the policy domain that contains the policy set.

You can delete the predefined STANDARD policy set. However, if you later reinstall the IBM Spectrum Protect™ server, the process restores all STANDARD policy objects.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-DELete POLicyset--domain_name--policy_set_name-------------><
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the policy set belongs.

policy_set_name (Required)
: Specifies the policy set to delete.

Example: Delete a policy set

Delete the VACATION policy set from the EMPLOYEE_RECORDS policy domain by issuing the following command:

```
delete policyset employee_records vacation
```

Related commands

Table 1. Commands related to DELETE POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY POLICYSET	Creates a copy of a policy set.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
QUERY POLICYSET	Displays information about policy sets.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

DELETE PROFASSOCIATION (Delete a profile association)

Use this command on a configuration manager to delete the association of one or more objects from a profile. If associations are deleted, the objects are no longer distributed to subscribing managed servers. When managed servers request updated configuration information, the configuration manager notifies them of the object deletions.

A managed server deletes the objects that were deleted from the profile, unless the objects are associated with another profile to which that server subscribes.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete PROFASSOCiation--profile_name------------------------->

>--+-------------------------------+---------------------------->
   '-ADMins--=--+-*--------------+-'
                | .-,----------. |
                | V            | |
                '---admin_name-+-'

>--+---------------------------------+-------------------------->
   '-DOmains--=--+-*---------------+-'
```

Parameters

profile_name (Required)
: Specifies the profile from which to delete associations.

ADMins
: Specifies the administrators whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all character (*) to delete all administrators from the profile. If you specify a list of administrators and a match-all definition exists for the profile, the command fails. Administrator definitions are not changed on the configuration manager. However, they are automatically deleted from all subscribing managed servers at the next configuration refresh, with the following exceptions:

  - An administrator is not deleted if that administrator has an open session on the server.
  - An administrator is not deleted if, as a result, the managed server would have no administrators with system privilege class.

DOmains
: Specifies the domains whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all character (*) to delete all domains from the profile. If you specify a list of domains and a match-all domain definition exists for the profile, the command fails.

  The domain information is automatically deleted from all subscribing managed servers. However, a policy domain that has client nodes assigned will not be deleted. To delete the domain at the managed server, assign those client nodes to another policy domain.

ADSCHeds
: Specifies a list of administrative schedules whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. If you specify a list of administrative schedules and a match-all administrative schedule definition exists for the profile, the command fails. Use the match-all character (*) to delete all administrative schedules from the profile.

  The administrative schedules are automatically deleted from all subscribing managed servers. However, an administrative schedule is not deleted if the schedule is active on the managed server. To delete an active schedule, make the schedule inactive.

SCRipts
: Specifies the server command scripts whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all character (*) to delete all scripts from the profile. If you specify a list of scripts and a match-all script definition exists for the profile, the command fails. The server command scripts are automatically deleted from all subscribing managed servers.

CLOptsets
: Specifies the client option sets whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. Use the match-all character (*) to delete all client option sets from the profile. If you specify a list of client option sets and a match-all client option set definition exists for the profile, the command fails. The client option sets are automatically deleted from all subscribing managed servers.

SERVers
: Specifies the servers whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. You can use the match-all character (*) to delete all servers from the profile. If you specify a list of servers and a match-all server definition exists for the profile, the command fails. The server definitions are automatically deleted from all subscribing managed servers with the following exceptions:

  - A server definition is not deleted if the managed server has an open connection to another server.
  - A server definition is not deleted if the managed server has a device class of the device type SERVER that refers to the other server.
  - A server definition is not deleted if the server is the event server for the managed server.

SERVERGroups
: Specifies the server groups whose association with the profile is deleted. You can specify more than one name by separating the names with commas and no intervening spaces. You can use the match-all character (*) to delete all server groups from the profile. If you specify a list of server groups and a match-all group definition exists for the profile, the command fails. The server group definitions are automatically deleted from all subscribing managed servers.

Example: Delete the domain associations for a specific profile

Delete all domain associations from a profile named MIKE.

```
delete profassociation mike domains=*
```

Related commands

Table 1. Commands related to DELETE PROFASSOCIATION

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

DELETE PROFILE (Delete a profile)

Use this command on a configuration manager to delete a profile and stop its distribution to managed servers.

You cannot delete a locked profile. You must first unlock the profile with the UNLOCK PROFILE command.

Deleting a profile from a configuration manager does not delete objects associated with that profile from the managed servers. You can use the DELETE SUBSCRIPTION command with the DISCARDOBJECTS=YES parameter on each subscribing managed

server to delete subscriptions to the profile and associated objects. This also prevents the managed servers from requesting further updates to the profile.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                                  .-Force--=--No------.
>>-DELete PROFIle--profile_name--+-------------------+---------><
                                  '-Force--=--+-No--+-'
                                              '-Yes-'
```

Parameters

profile_name (Required)
: Specifies the profile to delete.

Force
: Specifies whether the profile is deleted if one or more managed servers have subscriptions to that profile. The default is NO. Possible values are:

  No
  : Specifies that the profile is not deleted if one or more managed servers have subscriptions to that profile. You can delete the subscriptions on each managed server using the DELETE SUBSCRIPTION command.

  Yes
  : Specifies that the profile is deleted even if one or more managed servers have subscriptions to that profile. Each subscribing server continues to request updates for the deleted profile until the subscription is deleted.

Examples: Delete a profile

Delete a profile named BETA, even if one or more managed servers subscribe to it.

```
delete profile beta force=yes
```

Related commands

Table 1. Commands related to DELETE PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
LOCK PROFILE	Prevents distribution of a configuration profile.
QUERY PROFILE	Displays information about configuration profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

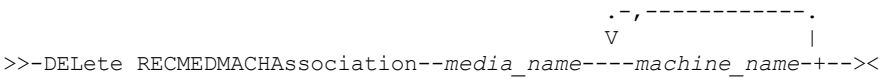
DELETE RECMEDMACHASSOCIATION (Delete recovery media and machine association)

Use this command to remove the association of one or more machines with a recovery media. This command does not delete the machine from IBM Spectrum Protect™.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

media_name (Required)
: Specifies the name of the recovery media that is associated with one or more machines.

machine_name (Required)
: Specifies the name of the machine associated with the recovery media. To specify a list of machine names, separate the names with commas and no intervening spaces. You can use wildcard characters to specify a name. If a machine is not associated with the recovery media, the machine is ignored.

Example: Delete a machine's association with recovery media

Delete the association between the DIST5RM recovery media and the DISTRICT1 and DISTRICT5 machines.

```
delete recmedmachassociation
dist5rm district1,district5
```

Related commands

Table 1. Commands related to DELETE RECMEDMACHASSOCIATION

Command	Description
DEFINE RECMEDMACHASSOCIATION	Associates recovery media with a machine.
QUERY MACHINE	Displays information about machines.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.

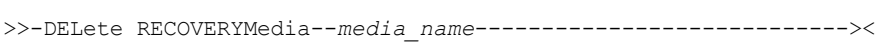
DELETE RECOVERYMEDIA (Delete recovery media)

Use this command to delete a recovery media definition from IBM Spectrum Protect™.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

media_name (Required)
Specifies the name of the recovery media.

Example: Delete a recovery media definition

Delete the DIST5RM recovery media.

```
delete recoverymedia dist5rm
```

Related commands

Table 1. Commands related to DELETE RECOVERYMEDIA

Command	Description
DEFINE RECOVERYMEDIA	Defines the media required to recover a machine.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.
UPDATE RECOVERYMEDIA	Changes the attributes of recovery media.

DELETE SCHEDULE (Delete a client or an administrative command schedule)

Use this command to delete schedules from the database.

The DELETE SCHEDULE command takes two forms: one if the schedule applies to client operations, one if the schedule applies to administrative commands. The syntax and parameters for each form are defined separately.

Table 1. Commands related to DELETE SCHEDULE

Command	Description
COPY SCHEDULE	Creates a copy of a schedule.
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
QUERY SCHEDULE	Displays information about schedules.
UPDATE SCHEDULE	Changes the attributes of a schedule.

- DELETE SCHEDULE (Delete a client schedule)
  Use the DELETE SCHEDULE command to delete one or more client schedules from the database. Any client associations to a schedule are removed when the schedule is deleted.
- DELETE SCHEDULE (Delete an administrative schedule)
  Use this command to delete one or more administrative command schedules from the database.

DELETE SCHEDULE (Delete a client schedule)

Use the DELETE SCHEDULE command to delete one or more client schedules from the database. Any client associations to a schedule are removed when the schedule is deleted.

Privilege class

To delete a client schedule, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the specified policy domain.

Syntax

```
>>-DELete SCHedule--domain_name--schedule_name------------------>

   .-Type--=--Client-.
```

```
>--+-----------------+-----------------------------------------><
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the schedule belongs.

schedule_name (Required)
: Specifies the name of the schedule to delete. You can use a wildcard character to specify this name.

Type=Client
: Specifies to delete a client schedule. This parameter is optional. The default is CLIENT.

Example: Delete a specific schedule from a specific policy domain

Delete the WEEKLY_BACKUP schedule, which belongs to the EMPLOYEE_RECORDS policy domain.

```
delete schedule employee_records weekly_backup
```

DELETE SCHEDULE (Delete an administrative schedule)

Use this command to delete one or more administrative command schedules from the database.

Privilege class

To delete an administrative command schedule, you must have system authority.

Syntax

```
>>-DELete SCHedule--schedule_name--Type--=--Administrative-----><
```

Parameters

schedule_name (Required)
: Specifies the name of the schedule to delete. You can use a wildcard character to specify this name.

Type=Administrative (Required)
: Specifies to delete an administrative command schedule.

Example: Delete an administrative command schedule

Delete the administrative command scheduled named DATA_ENG.

```
delete schedule data_eng type=administrative
```

DELETE SCRATCHPADENTRY (Delete a scratch pad entry)

Use this command to delete one or more lines of data from a scratch pad.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete SCRATCHPadentry--major_category--minor_category------->

            .-Line--=--*------.
>--subject--+-----------------+-------------------------------><
            '-Line--=--number-'
```

Parameters

major_category (Required)
: Specifies the major category from which one or more lines of data are to be deleted. This parameter is case sensitive.

minor_category (Required)
: Specifies the minor category from which one or more lines of data are to be deleted. This parameter is case sensitive.

subject (Required)
: Specifies the subject from which one or more lines of data are to be deleted. This parameter is case sensitive.

Line
: Specifies a line of data that is to be deleted. For number, enter the number of the line that is to be deleted. All data on the line is deleted. The numbering of other lines in the subject section is not affected. You can delete all lines of data from a subject section by omitting the Line parameter in this command.

Example: Delete all lines of data from a subject in a scratch pad

Delete all lines of data about the location of an administrator, Jane, from a database that stores information about administrators:

```
delete scratchpadentry admin_info location jane
```

Related commands

Table 1. Commands related to DELETE SCRATCHPADENTRY

Command	Description
DEFINE SCRATCHPADENTRY	Creates a line of data in the scratch pad.
QUERY SCRATCHPADENTRY	Displays information that is contained in the scratch pad.
SET SCRATCHPADRETENTION	Specifies the amount of time for which scratch pad entries are retained.
UPDATE SCRATCHPADENTRY	Updates data on a line in the scratch pad.

DELETE SCRIPT (Delete command lines from a script or delete the entire script)

Use this command to delete a single line from an IBM Spectrum Protect™ script or to delete the entire IBM Spectrum Protect script.

Privilege class

To issue this command, the administrator must have previously defined the script or must have system privilege.

Syntax

```
>>-DELete SCRipt--script_name--+-----------------+-------------><
                               '-Line--=--number-'
```

Parameters

script_name (Required)
: Specifies the name of the script to delete. The script is deleted unless you specify a line number.

Line
: Specifies the line number to delete from the script. If you do not specify a line number, the entire script is deleted.

Example: Delete a specific line from a script

Using the following script named QSAMPLE and issue a command to delete line 005 from it.

```
001  /* This is a sample script */
005  QUERY STATUS
010  QUERY PROCESS

delete script qsample line=5
```

Related commands

Table 1. Commands related to DELETE SCRIPT

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
QUERY SCRIPT	Displays information about scripts.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

DELETE SERVER (Delete a server definition)

Use this command to delete a server definition.

This command fails if the server:

- Is defined as the event server.
- Is named in a device class definition whose device type is SERVER.
- Has an open connection to or from another server.
- Is a target server for virtual volumes.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete--SERver--server_name---------------------------------><
```

Parameters

server_name (Required)
Specifies a server name.

Example: Delete a server's definition

Delete the definition for a server named SERVER2.

```
delete server server2
```

Related commands

Table 1. Commands related to DELETE SERVER

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.
QUERY EVENTSERVER	Displays the name of the event server.
QUERY SERVER	Displays information about servers.

Command	Description
RECONCILE VOLUMES	Reconciles source server virtual volume definitions and target server archive objects.
UPDATE SERVER	Updates information about a server.

DELETE SERVERGROUP (Delete a server group)

Use this command to delete a server group. If the group you delete is a member of other server groups, IBM Spectrum Protect™ also removes the group from the other groups.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete SERVERGroup--group_name-----------------------------><
```

Parameters

group_name (Required)
Specifies the server group to delete.

Example: Delete a server group

Delete a server group named WEST_COMPLEX.

```
delete servergroup west_complex
```

Related commands

Table 1. Commands related to DELETE SERVERGROUP

Command	Description
COPY SERVERGROUP	Creates a copy of a server group.
DEFINE GRPMEMBER	Defines a server as a member of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE GRPMEMBER	Deletes a server from a server group.
MOVE GRPMEMBER	Moves a server group member.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

DELETE SPACETRIGGER (Delete the storage pool space triggers)

Use this command to delete the definition of the storage pool space trigger.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-DELete SPACETrigger--STG------------------------------------>

>--+-----------------------------+-------------------------><
   '-STGPOOL--=--storage_pool_name-'
```

Parameters

STG
: Specifies a storage pool space trigger.

STGPOOL
: Specifies the storage pool trigger to be deleted. If STG is specified without specifying STGPOOL, the default storage pool space trigger is the deletion target.

Example: Delete a space trigger definition

Delete the space trigger definition for the WINPOOL1 storage pool.

```
delete spacetrigger stg stgpool=winpool1
```

Related commands

Table 1. Commands related to DELETE SPACETRIGGER

Command	Description
DEFINE SPACETRIGGER	Defines a space trigger to expand the space for a storage pool.
QUERY SPACETRIGGER	Displays information about a storage pool space trigger.
UPDATE SPACETRIGGER	Changes attributes of storage pool space trigger.

DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)

Use this command to delete an existing status monitoring threshold.

Status monitoring thresholds compare the defined conditions to the status monitoring server queries and inserts the results in the status monitoring table.

Multiple thresholds can be defined for an activity. For example, you can create a threshold that provides a warning status if storage pool capacity utilization is greater than 80%. You can then create another threshold that provides error status if storage pool capacity utilization is greater than 90%.

Note: If a threshold is already defined for an EXISTS condition, you cannot define another threshold with one of the other condition types.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete STAtusthreshold--threshold_name---------------------><
```

Parameters

threshold_name (Required)
: Specifies the threshold name that you want to delete.

Delete an existing status threshold

Delete an existing status threshold by issuing the following command:

```
delete statusthreshold avgstgpl
```

Related commands

Table 1. Commands related to DELETE STATUSTHRESHOLD

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

DELETE STGPOOL (Delete a storage pool)

Use this command to delete a storage pool. To delete a storage pool, you must first delete all volumes that are assigned to the storage pool.

You cannot delete a storage pool that is identified as the next storage pool for another storage pool. For more information about storage pool hierarchy, see the NEXTSTGPOOL parameter in the DEFINE STGPOOL command.

Restrictions:

- For container storage pools, delete all storage pool directories before you delete the storage pool.
- Do not delete a storage pool that is specified as a destination for a management class or copy group in the ACTIVE policy set. Client operations might fail as a result.
- When you delete a copy storage pool that was previously included in a primary storage-pool definition (specifically in the COPYSTGPOOLS list), you must remove the copy storage pool from the list before deletion. Otherwise, the DELETE STGPOOL command fails until all references to that copy pool are removed. For each primary storage pool with a reference to the copy storage pool to be deleted, remove the reference by entering the UPDATE STGPOOL command with the COPYSTGPOOLS parameter with all previous copy storage pools except the copy storage pool to be deleted.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete STGpool--pool_name-----------------------------------><
```

Parameters

pool_name (Required)
: Specifies the storage pool to delete.

Example: Delete a storage pool

Delete the storage pool named POOLA.

```
delete stgpool poola
```

Related commands

Table 1. Commands related to DELETE STGPOOL

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
DELETE STGPOOLDIRECTORY	Deletes a storage pool directory from a directory-container or cloud-container storage pool.
QUERY STGPOOL	Displays information about storage pools.
QUERY STGPOOLDIRECTORY	Displays information about storage pool directories.
AIX Windows SET DRMCOPYSTGPOOL	AIX Windows Specifies that copy storage pools are managed by DRM.
UPDATE STGPOOL	Changes the attributes of a storage pool.
UPDATE STGPOOLDIRECTORY	Changes the attributes of a storage pool directory.

DELETE STGPOOLDIRECTORY (Deleting a storage pool directory)

Use this command to delete a definition for a storage pool directory.

You might want to delete a storage pool directory for the following reasons:

- To decommission old storage.
- To discontinue using the local disk before moving data to the cloud.
- To no longer maintain the data in the storage pool directory because there is no requirement to do so.

Restrictions:

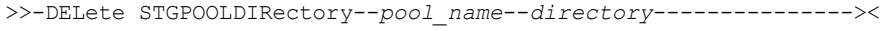
- You can issue this command only when no containers are assigned to the storage pool directory. Issue the QUERY CONTAINER command to determine whether any containers are assigned to the storage pool directory.
- To remove containers from a storage pool directory, you must issue the UPDATE STGPOOLDIRECTORY command and specify the ACCESS=DESTROYED parameter. Then, issue the AUDIT CONTAINER command and specify the ACTION=REMOVEDAMAGED parameter. Verify that the containers are removed.
  The ACTION=REMOVEDAMAGED parameter removes the inventory information of the objects that were backed up or archived. You should only remove the inventory information if you do not need the backups.

If you experience a hardware failure or a loss of your directory, see the relevant AUDIT and REPAIR commands. You should make any repairs to the IBM Spectrum Protect™ environment before you delete the storage pool directory.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

pool_name (Required)
: Specifies the storage pool that contains the directory to delete. This parameter is required.

directory (Required)
Specifies the file system directory of the storage pool to delete. This parameter is required.

Example: Update a storage pool directory to prepare for deletion

Update the storage pool directory that is named DIR1 in storage pool POOLA to mark as destroyed. When a storage pool is marked as destroyed, you can delete it.

AIX Linux

```
update stgpooldirectory poola /storage/dir1 access=destroyed
```

Windows

```
update stgpooldirectory poola e:\storage\dir1 access=destroyed
```

Example: Delete a storage pool directory

Delete the storage pool directory that is named DIR1 in storage pool POOLA.

AIX Linux

```
delete stgpooldirectory poola /storage/dir1
```

Windows

```
delete stgpooldirectory poola e:\storage\dir1
```

Table 1. Commands related to DELETE STGPOOLDIRECTORY

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
QUERY STGPOOLDIRECTORY	Displays information about storage pool directories.
UPDATE STGPOOLDIRECTORY	Changes the attributes of a storage pool directory.
QUERY EXTENTUPDATES	Displays information about updates to data extents in directory-container storage pools.

DELETE STGRULE (Delete storage rules for storage pools)

Use this command to delete storage rules for one or more storage pools.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete STGRULE--rule_name-----------------------------------><
```

Parameters

rule_name(Required)
Specifies the name of the storage rule that must be deleted. The maximum length of the name is 30 characters.

Delete a storage rule

Delete a storage rule that is named stgrule1:

```
delete stgrule stgrule1
```

Related commands

Table 1. Commands related to DELETE STGRULE

Command	Description
DEFINE STGRULE (tiering)	Defines a storage rule for tiering.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (tiering)	Updates a tiering storage rule.

DELETE SUBSCRIBER (Delete subscriptions from a configuration manager database)

Use this command on a configuration manager to delete managed server subscriptions from the configuration manager database. Use this command when a managed server no longer exists or cannot notify the configuration manager after deleting a subscription.

Attention: Use this command only in rare situations in which the configuration manager's database contains an entry for a subscription, but the managed server does not have such a subscription. For example, use this command if a managed server no longer exists or cannot notify the configuration manager after deleting a subscription.

Under normal circumstances, use the DELETE SUBSCRIPTION command to delete a subscription from the managed server. The managed server notifies the configuration manager, which then deletes the subscription from its database.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete SUBSCRIBer--server_name-----------------------------><
```

Parameters

server_name (Required)
Specifies the name of the managed server with subscription entries to be deleted.

Example: Delete subscription entries for a specific managed server

Delete all subscription entries for a managed server named DAN.

```
delete subscriber dan
```

Related commands

Table 1. Commands related to DELETE SUBSCRIBER

Command	Description
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.

DELETE SUBSCRIPTION (Delete a profile subscription)

Use this command on a managed server to delete a profile subscription. You can also delete from the managed server all objects associated with the profile.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DELete SUBSCRIPtion--profile_name---------------------------->

   .-DISCARDobjects--=--No------.
>--+----------------------------+------------------------------><
   '-DISCARDobjects--=--+-No--+-'
                        '-Yes-'
```

Parameters

profile_name (Required)
: Specifies the name of the profile for which the subscription is to be deleted.

DISCARDobjects
: Specifies whether objects associated with the profile are to be deleted on the managed server. This parameter is optional. The default is NO.

  No
  : Specifies that the objects are not to be deleted.

  Yes
  : Specifies that the objects are to be deleted, unless they are associated with another profile for which a subscription is defined.

Example: Delete a profile subscription

Delete a subscription to a profile named ALPHA and its associated objects from a managed server.

```
delete subscription alpha discardobjects=yes
```

Related commands

Table 1. Commands related to DELETE SUBSCRIPTION

Command	Description
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.

DELETE VIRTUALFSMAPPING (Delete a virtual file space mapping)

Use this command to delete a virtual file space mapping definition. Virtual file spaces containing data cannot be deleted unless you use the DELETE FILESPACE command first.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege
- Restricted policy privilege for the domain to which the NAS node is assigned

Syntax

```
>>-DELete VIRTUALFSmapping  -node_name-------------------------->

>--virtual_filespace_name---------------------------------------><
```

Parameters

node_name (Required)
: Specifies the NAS node on which the file system and path reside. You cannot use wildcard characters or specify a list of names.

virtual_filespace_name (Required)
: Specifies the name of the virtual file space mapping definition to be deleted. Wildcard characters are allowed.

Example: Delete a virtual file space mapping

Delete the virtual file space mapping definition /mikeshomedir for the NAS node named NAS1.

```
delete virtualfsmapping nas1 /mikeshomedir
```

Related commands

Table 1. Commands related to DELETE VIRTUALFSMAPPING

Command	Description
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
QUERY VIRTUALFSMAPPING	Query a virtual file space mapping.
UPDATE VIRTUALFSMAPPING	Update a virtual file space mapping.

DELETE VOLHISTORY (Delete sequential volume history information)

Use this command to delete volume history file records that are no longer needed (for example, records for obsolete database backup volumes).

When you delete records for volumes that are not in storage pools (for example, database backup or export volumes), the volumes return to scratch status even if IBM Spectrum Protect™ acquired them as private volumes. Scratch volumes of device type FILE are deleted. When you delete the records for storage pool volumes, the volumes remain in the IBM Spectrum Protect database. When you delete records for recovery plan file objects from a source server, the objects on the target server are marked for deletion.
Restriction: Do not use the DELETE VOLHISTORY command to delete information about backup set volumes from the volume history file. Instead, use the DELETE BACKUPSET command for this purpose.

For users of DRM, the database backup expiration should be controlled with the SET DRMDBBACKUPEXPIREDAYS command instead of this DELETE VOLHISTORY command. Use the DELETE VOLHISTORY command to remove a record of the volume. This can cause volumes to be lost that were managed by the MOVE DRMEDIA command. Use the SET DRMDBBACKUPEXPIREDAYS command to manage the automatic expiration of DRM database backup volumes.

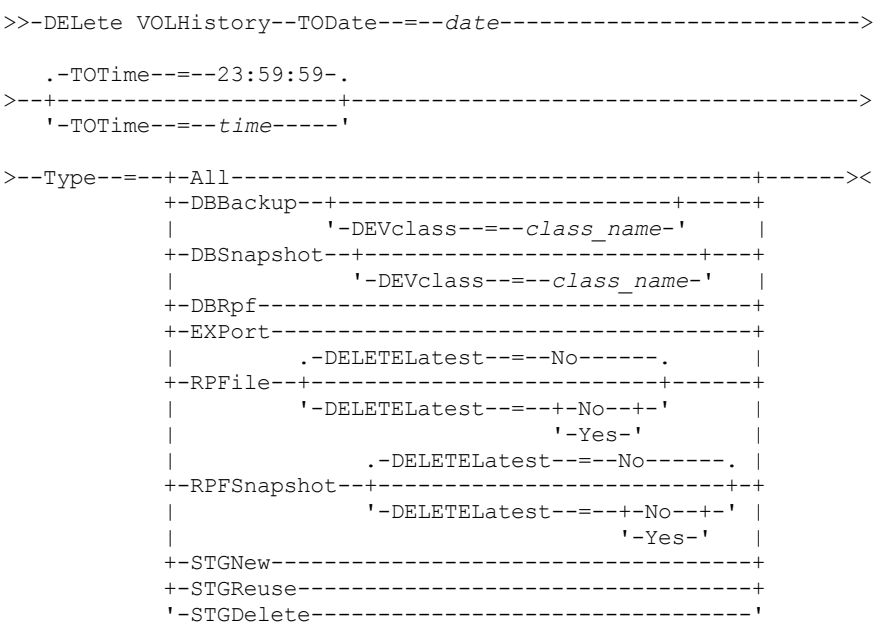
Tips:

- Volumes for the most recent database backup series are not deleted.
- Existing volume history files are not automatically updated with this command.
- You can use the DEFINE SCHEDULE command to periodically delete volume history records.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

TODate (Required)

Specifies the date to use to select sequential volume history information to be deleted. You can delete only those records with a date on or before the date that you specify. You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	01/23/1999
TODAY	The current date	TODAY
TODAY-days or -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–30 or –30. To delete records that are 30 or more days old, you can specify TODAY-30 or simply -30.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

TOTime

Specifies that you want to delete records that are created on or before this time on the specified date. This parameter is optional. The default is the end of the day (23:59:59). You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified date	12:30:22
NOW	The current time on the specified date	NOW

Value	Description	Example
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified date	NOW+03:00 or +03:00. If you issue the DELETE VOLHISTORY command at 9:00 with TOTIME=NOW+03:00 or TOTIME=+03:00, IBM Spectrum Protect deletes records with a time of 12:00 or earlier on the specified date.
NOW-HH:MM or -HH:MM	The current time minus hours and minutes on the specified date	NOW-03:30 or -03:30. If you issue the DELETE VOLHISTORY command at 9:00 with TOTIME=NOW-3:30 or TOTIME=-3:30, IBM Spectrum Protect deletes records with a time of 5:30 or earlier on the specified date.

Type (Required)

Specifies the type of records, which also meet the date and time criteria, to delete from the volume history file. Possible values are:

All

Specifies to delete all records.
Restriction: The DELETE VOLHISTORY command does not delete records of remote volumes.

DBBackup

Specifies to delete only records that contain information about volumes that are used for database full and incremental backups, that is, with volume types of BACKUPFULL and BACKUPINCR, and that meet the specified date and time criteria. The records from the latest full and incremental database backup series will not be deleted.

DEVclass=class_name

Specifies the device class name that was used to create the database backups. This optional parameter can be used to delete database backups that are created by using a server-to-server virtual volume device class. The type of the device class must be SERVER. This parameter can be used only to delete volume history entries of type BACKUPFULL, BACKUPINCR, or DBSNAPSHOT.
A full or incremental database backup volume is eligible to be deleted if all of the following conditions are met:

- The device class that was used to create the database backup volume matches the specified device class.
- The volume was created on or before the specified date and time.
- The volume is not part of the latest full plus incremental database backup series.
- The volume is not part of a full plus incremental backup series with an incremental database backup that was created after the specified date and time.

DBSnapshot

Specifies to delete only records that contain information about volumes that are used for snapshot database backups, and that meet the specified date and time criteria. Records that are related to the latest snapshot database backup will not be deleted.

DEVclass=classname

Specifies the device class name that was used to create the database backups. This optional parameter can be used to delete database backups that are created by using a server-to-server virtual volume device class. The type of the device class must be SERVER. This parameter can only be used to delete volume history entries of type BACKUPFULL, BACKUPINCR, or DBSNAPSHOT.
A snapshot database backup volume is eligible to be deleted if all of the following conditions are met:

- The device class that is used to create the database backup volume matches the specified device class
- The volume was created on or before the specified date and time
- The volume is not part of the latest snapshot database backup series

DBRpf

Specifies to delete only records that contain information about full and incremental database backup volumes and recovery plan file volumes.

EXPort

Specifies to delete only records that contain information about export volumes.

RPFile
: Specifies to delete only records that contain information about recovery plan file objects that are stored on a target server and that meet the specified date and time criteria.

  DELETELatest
  : Specifies whether the latest recovery plan file is eligible for deletion. This optional parameter can be used to delete the latest recovery plan files that are created by using a server-to-server virtual volume device class.

    This parameter can be used only to delete volume history entries of type RPFILE (for instance, those recovery plan files that were created by using the DEVCLASS parameter with the PREPARE command). If this parameter is not specified, the latest RPFILE entries are not deleted.

    No
    : Specifies the latest RPFILE file is not deleted.

    Yes
    : Specifies the latest RPFILE file is deleted if it meets the specified date and time criteria.

RPFSnapshot
: Specifies to delete only records that contain information about recovery plan file objects that were created for snapshot database backups, that are stored on a target server and that meet the specified date and time criteria. The latest RPFSNAPSHOT file will not be deleted unless it meets the specified date and time criteria, and the DELETE parameter is set to Yes.

  DELETELatest
  : Specifies whether the latest recovery plan file is eligible for deletion. This optional parameter can be used to delete the latest recovery plan files that are created by using a server-to-server virtual volume device class.

    This parameter can only be used to delete volume history entries of type RPFSNAPSHOT (for instance, those recovery plan files that were created by using the DEVCLASS parameter with the PREPARE command). If this parameter is not specified, the latest RPFSNAPSHOT entries are not deleted.

    No
    : Specifies the latest RPFSNAPSHOT file is not deleted.

    Yes
    : Specifies the latest RPFSNAPSHOT file is deleted if it meets the specified date and time criteria.

STGNew
: Specifies to delete only records that contain information about new sequential access storage volumes.

STGReuse
: Specifies to delete only records that contain information about reused sequential storage pool volumes.

STGDelete
: Specifies to delete only records that contain information about deleted sequential storage pool volumes.

Example: Delete recovery plan file information

Delete all recovery plan file information that is created on or before 03/28/2016.

```
delete volhistory type=rpfile todate=03/28/2016
```

Related commands

Table 1. Commands related to DELETE VOLHISTORY

Command	Description
BACKUP VOLHISTORY	Records volume history information in external files.
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
DELETE VOLUME	Deletes a volume from a storage pool.
EXPIRE INVENTORY	Manually starts inventory expiration processing.
MOVE DRMEDIA	Moves DRM media onsite and offsite.

Command	Description
PREPARE	Creates a recovery plan file.
QUERY RPFILE	Displays information about recovery plan files.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
SET DRMRPFEXPIREDAYS	Set criteria for recovery plan file expiration.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.

DELETE VOLUME (Delete a storage pool volume)

Use this command to delete a storage pool volume and, optionally, the files stored in the volume.

If the volume has data, to delete the volume you must do one of the following:

- Before deleting the volume, use the MOVE DATA command to move all files to another volume.
- Explicitly request to discard all files in the volume when the volume is deleted (by specifying DISCARDDATA=YES).

If you are deleting several volumes, delete the volumes one at a time. Deleting more than one volume at a time can adversely affect server performance.

Storage pool volumes cannot be deleted if they are in use. For example, a volume cannot be deleted if a user is restoring or retrieving a file residing in the volume, if the server is writing information to the volume, or if a reclamation process is using the volume.

If you issue the DELETE VOLUME command, volume information is deleted from the IBM Spectrum Protect™ database. However, the physical files that are allocated with DEFINE VOLUME command are not removed from the file space.

If this command is applied to a WORM (write once, read many) volume, the volume returns to scratch if it has space remaining in which data can be written. Data on WORM volumes, including deleted and expired data, cannot be overwritten. Therefore, data can only be written in space that does not contain current, deleted, or expired data. If a WORM volume does not have any space available in which data can be written, it remains private. To remove the volume from the library, you must use the CHECKOUT LIBVOLUME command.

The DELETE VOLUME command automatically updates the server library inventory for sequential volumes if the volume is returned to scratch status when the volume becomes empty. To determine whether a volume will be returned to scratch status, issue the QUERY VOLUME command and look at the output. If the value for the attribute "Scratch Volume?" is "Yes," then the server library inventory is automatically updated.

If the value is "No," you can issue the UPDATE LIBVOLUME command to specify the status as scratch. It is recommended that you issue the UPDATE LIBVOLUME command after issuing the DELETE VOLUME command.

Attempting to use the DELETE VOLUME command to delete WORM FILE volumes in a storage pool with RECLAMATIONTYPE=SNAPLOCK fails with an error message. Deletion of empty WORM FILE volumes is performed only by the reclamation process.

If you issue the DELETE VOLUME command for a volume in a storage pool that has a SHRED parameter value greater than 0, the volume is placed in the pending state until shredding is run. Shredding is necessary to complete the deletion, even if the volume is empty.

If you issue the DELETE VOLUME command for a volume in a storage pool that is set up for data deduplication, the server destroys any object that is referencing data on that volume.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to which the volume is defined.

Syntax

```
.-DISCARDdata--=--No------.
```

```
>>-DELete Volume--volume_name--+-------------------------+------>
                               '-DISCARDdata--=--+-No--+-'
                                                 '-Yes-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameters

volume_name (Required)
: Specifies the name of the volume to delete.

DISCARDdata
: Specifies whether files stored in the volume are deleted. This parameter is optional. The default value is NO. Possible values are:

  No
  : Specifies that files stored in the volume are not deleted. If the volume contains any files, the volume is not deleted.

  Yes
  : Specifies that all files stored in the volume are deleted. The server does not need to mount the volume for this type of deletion.
  Remember:

    1. The server does not delete archive files that are on deletion hold.
    2. If archive retention protection is enabled, the server deletes only archive files whose retention period has expired.

  If the volume being deleted is a primary storage pool volume, the server checks whether any copy storage pool has copies of files that are being deleted. When files stored in a primary storage pool volume are deleted, any copies of these files in copy storage pools are also deleted.

  When you delete a disk volume in a primary storage pool, the command also deletes any files that are cached copies (copies of files that have been migrated to the next storage pool). Deleting cached copies of files does not delete the files that have already been migrated or backed up to copy storage pools. Only the cached copies of the files are affected.

  If the volume being deleted is a copy storage pool volume, only files on the copy pool volume are deleted. The primary storage pool files are not affected.

  Do not use the DELETE VOLUME command with DISCARDDATA=YES if a restore process (RESTORE STGPOOL or RESTORE VOLUME) is running. The DELETE VOLUME command could cause the restore to be incomplete.

  If you cancel the DELETE VOLUME operation during processing or if a system failure occurs, some files might remain on the volume. You can delete the same volume again to have the server delete the remaining files and then the volume.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter affects processing only when you have also requested that any data on the volume be discarded. This parameter is optional. The default value is No. Possible values are:

  No
  : Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

  The server displays messages that are created from the background process either in the activity log or the server console, depending on where messages are logged.

  Yes
  : Specifies that the server processes this command in the foreground. You wait for the command to complete before continuing with other tasks. The server then displays the output messages to the administrative client when the command completes.
  Remember: You cannot specify WAIT=YES from the server console.

Example: Delete a storage pool volume

Delete storage pool volume stgvol.1 from the storage pool FILEPOOL.

```
delete volume stgvol.1
```

Related commands

Table 1. Commands related to DELETE VOLUME

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
MOVE DATA	Moves data from a specified storage pool volume to another storage pool volume.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY PROCESS	Displays information about background processes.
QUERY VOLUME	Displays information about storage pool volumes.
UPDATE VOLUME	Updates the attributes of storage pool volumes.

DISABLE commands

Use DISABLE commands to prevent some types of operations by the server.

- DISABLE EVENTS (Disable events for event logging)
- DISABLE REPLICATION (Prevent outbound replication processing on a server)
- DISABLE SESSIONS (Prevent new sessions from accessing IBM Spectrum Protect)

DISABLE EVENTS (Disable events for event logging)

Use this command to disable the processing of one or more events. If you specify a receiver that is not supported on any platform, or if you specify an invalid event or name, IBM Spectrum Protect™ issues an error message. However, any valid receivers, events, or names that you specified are still enabled.

Tip: Messages in the SEVERE category and message ANR9999D can provide valuable diagnostic information if there are serious server problems. For this reason, you should not disable these messages.
Restriction:

- Certain messages are displayed on the console even if they are disabled. These include some messages issued during server startup and shutdown and responses to administrative commands.
- Server messages from the server on which this command is issued cannot be disabled for the activity log.

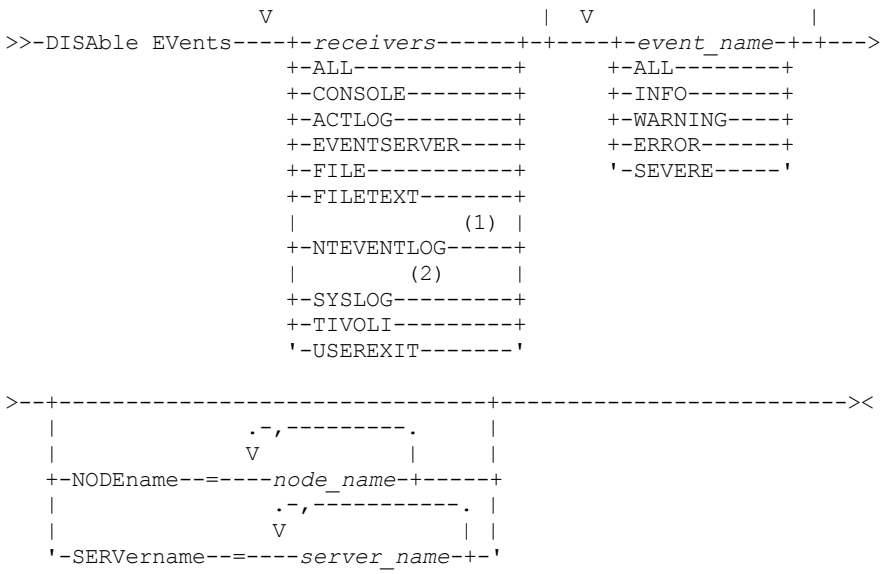
ANR1822I indicates that event logging is being ended for the specified receiver. When the DISABLE EVENTS command is issued, this message is logged to the receiver even if it is one of the events that has been disabled. This is done to confirm that event logging has ended to that receiver, but subsequent ANR1822I messages are not logged to that receiver.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                .-,------------------.   .-,--------------.
```



Notes:

1. NTEVENTLOG is available only on Windows.
2. SYSLOG is available only on Linux.

Parameters

receivers (Required)
: Specifies the name of the receivers for which to disable events. Specify multiple receivers by separating them with commas and no intervening spaces. Possible values are:

  ALL
  : All receivers, except for server events on the activity log receiver (ACTLOG). Only client events can be disabled for the activity log receiver.

  CONSOLE
  : The standard server console as a receiver.

  ACTLOG
  : The activity log as a receiver. You can disable only client events, not server events, for the activity log.

  EVENTSERVER
  : The event server as a receiver.

  FILE
  : A user file as a receiver. Each logged event is a record in the file. The records are not easily readable by people.

  FILETEXT
  : A user file as a receiver. Each logged event is a fixed-size, readable line.

  NTEVENTLOG
  : The Windows application log as a receiver.

  Linux SYSLOG
  : Linux Writes messages directly to the system log on Linux.

  TIVOLI
  : The Tivoli Enterprise Console® (TEC) as a receiver.

  USEREXIT
  : A user-written program as a receiver. The server writes information to the program.

events (Required)
: Specifies the events to be disabled. You can specify multiple events by separating them with commas and no intervening spaces. Possible values are:

  ALL
  : All events.

  event_name
  : A four-digit message number preceded by ANR for a server event or ANE for a client event. Valid ranges are from ANR0001 to ANR9999 and from ANE4000 to ANE4999. Specify the NODENAMES parameter if client events are to

be disabled for matching nodes. Specify the SERVERNAME parameter if server events are to be disabled for matching servers.
For the TIVOLI event receiver only, you can specify the following events names for the IBM Spectrum Protect application clients:

IBM Spectrum Protect application client	Prefix	Range
Data Protection for Microsoft Exchange Server	ACN	3500–3649
Data Protection for Lotus® Domino®	ACD	5200–5299
Data Protection for Oracle	ANS	500–599
Data Protection for Informix®	ANS	600–699
Data Protection for Microsoft SQL Server	ACO	3000–3999

Remember: Specifying ALL disables these messages. However, the INFO, WARNING, ERROR, and SEVERE options have no effect on the messages.

severity categories
If the event list contains a severity category, all events of that severity are disabled for the specified nodes. The message types are:

INFO
Information messages (type of I).
WARNING
Warning messages (type of W).
ERROR
Error messages (type of E).
SEVERE
Severe error messages (type of S).

NODEname
Specifies the name of one or more node names for which events are to be disabled. You can use the wildcard character (*) to specify all nodes. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the events are disabled for the server running this command.

SERVername
Specifies the name of one or more server names for which events are to be disabled. You can use the wildcard character (*) to specify all servers other than the server running this command. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the events are disabled for the server running this command.

Example: Disable specific categories of events

Disable all client events in the INFO and WARNING categories for the activity log and console receivers for all nodes.

```
disable events actlog,console
info,warning nodename=*
```

Related commands

Table 1. Commands related to DISABLE EVENTS

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
ENABLE EVENTS	Enables specific events for receivers.
END EVENTLOGGING	Ends event logging to a specified receiver.
QUERY ENABLED	Displays enabled or disabled events for a specific receiver.
QUERY EVENTRULES	Displays information about rules for server and client events.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

DISABLE REPLICATION (Prevent outbound replication processing on a server)

Use this command to prevent a source replication server from starting new replication processes.

The use of this command does not stop running replication processes. Running replication processes continue until they complete or until they end without completing. Use this command and the ENABLE REPLICATION command to control replication processing.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-DISAble REPLication-----------------------------------------><
```

Parameters

None.

Example: Disable replication processing

Disable replication processing on a source replication server.

```
disable replication
```

Related commands

Table 1. Commands related to DISABLE REPLICATION

Command	Description
CANCEL REPLICATION	Cancels node replication processes.
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
ENABLE REPLICATION	Allows outbound replication processing on a server.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.

DISABLE SESSIONS (Prevent new sessions from accessing IBM Spectrum Protect)

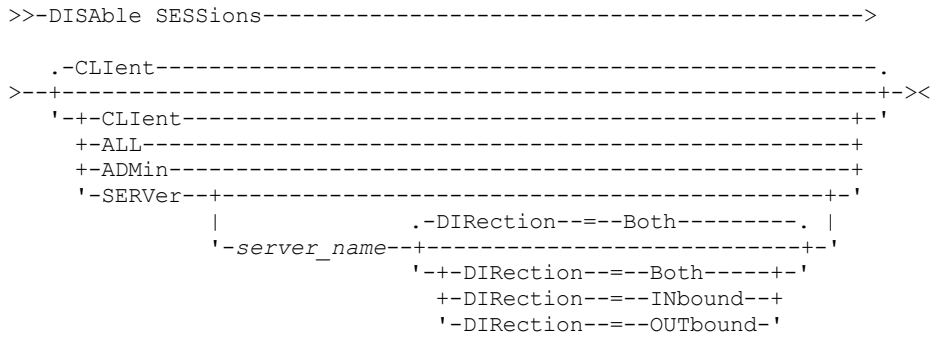
Use this command to prevent new sessions from accessing IBM Spectrum Protect™. Active sessions will complete. For a particular server, you can specify whether to disable inbound sessions, outbound sessions, or both.

Server processes, such as migration and reclamation, are not affected when you issue the DISABLE SESSIONS command.

Privilege class

To issue this command, you must have system privilege or operator privilege.

Syntax



Parameters

Specifies the type of session to be disabled. This parameter is optional. The default value is CLIENT. You can specify one of the following values:

CLIent
: Disables only backup and archive client sessions.

ALL
: Disables all session types.

ADMin
: Disables only administrative sessions.

SERVer
: Disables only server-to-server sessions. Only the following types of sessions are disabled:

  - Server-to-server event logging
  - Enterprise management
  - Server registration
  - LAN-free: storage agent - server
  - Virtual volumes
  - Node replication

  You can also specify whether to disable inbound sessions, outbound sessions, or both for a particular server.

  server_name
  : Specifies the name of a server whose sessions you want to disable. This parameter is optional. If you do not specify this parameter, new sessions with other servers do not start. Running sessions are not canceled.

    DIRection
    : Specifies whether to disable inbound sessions, outbound sessions, or both. This parameter is optional. The default is BOTH. The following values are possible:

      Both
      : Specifies that inbound sessions from the specified server and outbound sessions to the specified server are disabled.

      INbound
      : Specifies that only inbound sessions from the specified server are disabled.

      OUTbound
      : Specifies that only outbound sessions to the specified server are disabled.

Example: Prevent new client node backup and archive sessions on the server

Temporarily prevent new client node sessions from accessing the server.

```
disable sessions
```

Example: Prevent all new sessions on the server

Temporarily prevent any new sessions from accessing the server.

```
disable sessions all
```

Example: Disable outbound sessions to a server

Disable outbound sessions to a server named REPLSRV.

```
disable sessions server replsrv direction=outbound
```

Related commands

Table 1. Commands related to DISABLE SESSIONS

Command	Description
CANCEL SESSION	Cancels active sessions with the server.
DISABLE REPLICATION	Prevents outbound replication processing on a server.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

DISMOUNT command

Use the DISMOUNT command to dismount a volume by the real device address or by volume name.

- DISMOUNT VOLUME (Dismount a volume by volume name)

DISPLAY OBJNAME (Display a full object name)

Use this command when you want IBM Spectrum Protect™ to display a full object name if the name displayed in a message or query output has been abbreviated due to length. Object names that are very long can be difficult to display and use through normal operating system facilities. The IBM Spectrum Protect server will abbreviate long names and assign them a token ID which might be used if the object path name exceeds 1024 bytes. The token ID is displayed in a string that includes identifiers for the node, filespace, and object name. The format is: [TSMOBJ:*nID.fsID.objID*]. When specified with the DISPLAY OBJNAME command, the token ID can be used to show the full object name.

Privilege class

Any administrator can issue this command

Syntax

```
>>-DISplay OBJname--token_ID-----------------------------------><
```

Parameters

token_ID (Required)
Specifies the ID reported in the [TSMOBJ:] tag, when an object name is too long to display.

Example: Display the full object name of a token ID in a message

Assume the you receive the following message:

```
ANR9999D file.c(1999) Error handling file [TSMOBJ:1.1.649498] because
of lack of server resources.
```

Display the full object name for the file referenced in the error message by specifying the token ID on the DISPLAY OBJNAME command.

```
display obj 1.1.649498
```

Related commands

Table 1. Commands related to DISPLAY OBJNAME

Command	Description
QUERY CONTENT	Displays information about files in a storage pool volume.

ENABLE commands

Use ENABLE commands to allow some types of operations by the server.

- ENABLE EVENTS (Enable server or client events for logging)
- ENABLE REPLICATION (Allow outbound replication processing on a server)
- ENABLE SESSIONS (Resume user activity on the server)

ENABLE EVENTS (Enable server or client events for logging)

Use this command to enable the processing of one or more events. If you specify a receiver that is not supported on any platform, or if you specify an invalid event or name, IBM Spectrum Protect™ issues an error message. However, any valid receivers, events, or names that you specified are still enabled.

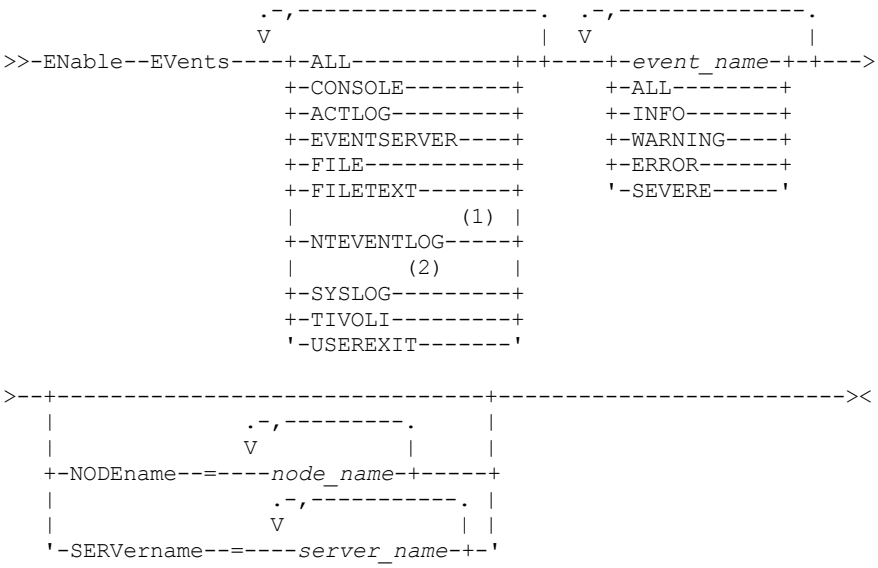
Restriction: Certain events, such as some messages issued during server start-up and shutdown, automatically go to the console. They do not go to other receivers even if they are enabled.

Administrative commands are returned to the command issuer and are only logged as numbered events. These numbered events are not logged to the system console, but are logged to other receivers, including administrative command-line sessions running in console mode.

Privilege class

To issue this command, you must have system privilege.

Syntax



Notes:

1. NTEVENTLOG is available only on Windows.
2. This parameter is only available for the Linux operating system.

Parameters

receivers (Required)

Specifies one or more receivers for which to log enabled events. You can specify multiple receivers by separating them with commas and no intervening spaces. Valid values are:

ALL
: All receivers.

CONSOLE
: The standard server console as a receiver.

ACTLOG
: The server activity log as a receiver.

EVENTSERVER
: The event server as a receiver.

FILE
: A user file as a receiver. Each logged event is a record in the file. The records are not easily readable by people.

FILETEXT
: A user file as a receiver. Each logged event is a fixed-size, readable line.

Windows NTEVENTLOG
: Windows The Windows application log as a receiver.

Linux SYSLOG
: Linux Specifies the Linux system log as a receiver with a facility of LOG_USER.

TIVOLI
: The Tivoli Enterprise Console® (TEC) as a receiver.

USEREXIT
: A user-written program as a receiver. The server writes information to the program.

events (Required)

Specifies the type of events to be enabled. You can specify multiple events by separating them with commas and no intervening spaces. Possible values are:

ALL
: All events.

event_name
: A four-digit message number preceded by `ANR` for a server event or `ANE` for a client event. Valid ranges are from ANR0001 to ANR9999 and from ANE4000 to ANE4999. Specify the NODENAME parameter if client events are to be enabled for matching nodes. Specify the SERVERNAME parameter if server events are to be enabled for matching servers.
  For the TIVOLI event receiver, you can specify the following additional ranges for the IBM Spectrum Protect application clients:

IBM Spectrum Protect application client	Prefix	Range
Data Protection for Microsoft Exchange Server	ACN	3500–3649
Data Protection for Lotus® Domino®	ACD	5200–5299
Data Protection for Oracle	ANS	500–599
Data Protection for Informix®	ANS	600–699
Data Protection for Microsoft SQL Server	ACO	3000–3999

  Restriction: The application client must have enhanced Tivoli® Event Console support enabled in order to route these messages to the Tivoli Event Console.
  Tip:

  - Specifying the ALL option enables these messages. However, the INFO, WARNING, ERROR, and SEVERE options have no effect on the messages.
  - Because of the number of messages, you should not enable all messages from a node to be logged to the Tivoli Event Console.

severity categories

If the event list contains a severity category, all events of that severity are enabled for the specified nodes. The message types are:

INFO
: Information messages (type of I) are enabled.

WARNING
: Warning messages (type of W) are enabled.

ERROR
: Error messages (type of E) are enabled.

SEVERE
: Severe error messages (type of S) are enabled.

NODEname
: Specifies one or more client nodes for which events are enabled. You can use a wildcard character to specify all client nodes. You can specify NODENAME or SERVERNAME. If neither parameter is specified, events are enabled for the server running this command.

SERVername
: Specifies one or more servers for which events are to be enabled. You can use a wildcard character to specify all servers other than the server from which this command is issued. You can specify SERVERNAME or NODENAME. If neither parameter is specified, the events are enabled for the server running this command.

Example: Enable specific categories of events

Enable all ERROR and SEVERE client events to the USEREXIT receiver for the node BONZO.

```
enable events userexit error,severe nodename=bonzo
```

Related commands

Table 1. Commands related to ENABLE EVENTS

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DISABLE EVENTS	Disables specific events for receivers.
END EVENTLOGGING	Ends event logging to a specified receiver.
QUERY ENABLED	Displays enabled or disabled events for a specific receiver.
QUERY EVENTRULES	Displays information about rules for server and client events.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

ENABLE REPLICATION (Allow outbound replication processing on a server)

Use this command to allow a source replication server to begin normal replication processing after a database restore. You can also use this command to resume replication processing after issuing the DISABLE REPLICATION command.

Attention: Before enabling replication after a database restore, determine whether copies of data that are on the target server are needed. If they are, you must synchronize client node data by replicating the data from the target replication server to the source replication server. The replication process replaces the data on the source server that was lost because of the database restore.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-ENable REPLication-----------------------------------------><
```

Parameters

None.

Example: Allow replication processing

Allow replication processing on a source replication server.

```
enable replication
```

Related commands

Table 1. Commands related to ENABLE REPLICATION

Command	Description
DISABLE REPLICATION	Prevents outbound replication processing on a server.
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.

ENABLE SESSIONS (Resume user activity on the server)

Use this command after issuing the DISABLE SESSIONS command to start new sessions that can access a server. For a particular server, you can specify whether to enable inbound sessions, outbound sessions, or both.

The processing of this command does not affect system processes, such as migration and reclamation.

Use the QUERY STATUS command to display the availability of the server.

Privilege class

To issue this command, you must have system privilege or operator privilege.

Syntax

```
>>-ENable SESSions---------------------------------------------->

   .-CLIent-------------------------------------------------------.
>--+-------------------------------------------------------------+-><
   '-+-CLIent-----------------------------------------------+-'
     +-ALL------------------------------------------------+
     +-ADMin----------------------------------------------+
     '-SERVer--+----------------------------------------+-'
               |              .-DIRection--=--Both---------. |
               '-server_name--+---------------------------+-'
                              '-+-DIRection--=--Both-----+-'
                                +-DIRection--=--INbound--+
                                '-DIRection--=--OUTbound-'
```

Parameters

Specifies the type of session to be enabled. This parameter is optional. The default value is CLIENT. You can specify one of the following values:

CLIent
: Enables only backup and archive client sessions.

ALL
: Enables all session types.

ADMin
: Enables only administrative sessions.

SERVer
: Enables only server-to-server sessions. You can also specify whether to enable inbound sessions, outbound sessions, or both for a particular server.

server_name
: Specifies the name of a particular server whose sessions you want to enable. This parameter is optional. If you do not specify this parameter, new sessions with all other servers are enabled.

DIRection
: Specifies whether to enable inbound sessions, outbound sessions, or both. This parameter is optional. The default is BOTH. The following values are possible:

Both
: Specifies that inbound sessions from the specified server and outbound sessions to the specified server are enabled.

INbound
: Specifies that only inbound sessions to the specified server are enabled.

OUTbound
: Specifies that only outbound sessions from the specified server are enabled.

Example: Resume client node activity on the server

Resume normal operation, permitting client nodes to access the server.

```
enable sessions
```

Example: Resume all activity on the server

Resume normal operation, permitting all sessions to access the server.

```
enable sessions all
```

Example: Enable outbound sessions to a server

Enable outbound sessions to a server named REPLSRV.

```
enable sessions server replsrv direction=outbound
```

Related commands

Table 1. Commands related to ENABLE SESSIONS

Command	Description
ACCEPT DATE	Accepts the current date on the server.
CANCEL SESSION	Cancels active sessions with the server.
ENABLE REPLICATION	Allows outbound replication processing on a server.
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

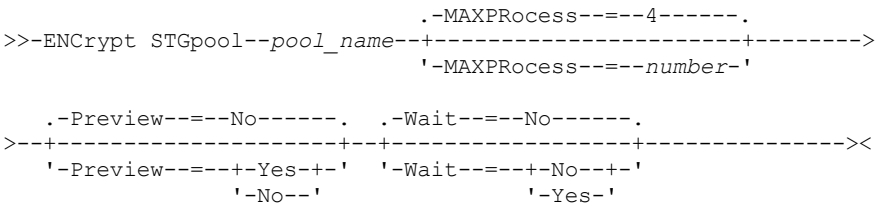
ENCRYPT STGPOOL (Encrypt data in a storage pool)

Use this command to encrypt data in a directory-container or cloud-container storage pool.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

pool_name (Required)
: Specifies the name of the storage pool that contains data that must be encrypted.
Restrictions:

- You can specify only directory-container storage pools or cloud-container storage pools.
- You can specify up to 30 characters for the storage pool name. If you specify more than 30 characters, the command fails.

MAXPRocess
: Specifies the maximum number of parallel processes that can occur when the storage pool is encrypting data. This parameter is optional. Enter a value in the range 1 - 99. The default value is 4.

Preview
: Specifies whether a preview is displayed of all the commands that are processed as part of the ENCRYPT STGPOOL command. This parameter is optional. The following values are possible:

  No
  : Specifies that a preview of the commands is not displayed. This is the default value.

  Yes
  : Specifies that a preview of the commands is displayed.

Wait
: Specifies whether the storage pool encryption occurs in the foreground or background. This parameter is optional. You can specify one of the following values:

  No
  : Specifies that the operation is completed in the background. You can continue with other tasks while the command is processing. Messages that are related to the background process are displayed in the activity log file or the server console, depending on where the messages are logged. This is the default value.

  Yes
  : Specifies that the operation is completed in the foreground. It might take a long time to complete the operation. The operation must end before you can continue with other tasks. Messages are displayed in the activity log file or the server console, or both, depending on where the messages are logged.
  Restriction: You cannot specify the WAIT=YES parameter from the server console.

Example: Encrypt data in a storage pool

Encrypt data in a storage pool that is named POOL1 and specify a maximum number of 30 parallel processes.

```
encrypt stgpool pool1 maxprocess=30
```

Related commands

Table 1. Commands related to ENCRYPT STGPOOL

Command	Description
DEFINE STGPOOL (directory-container)	Define a directory-container storage pool.

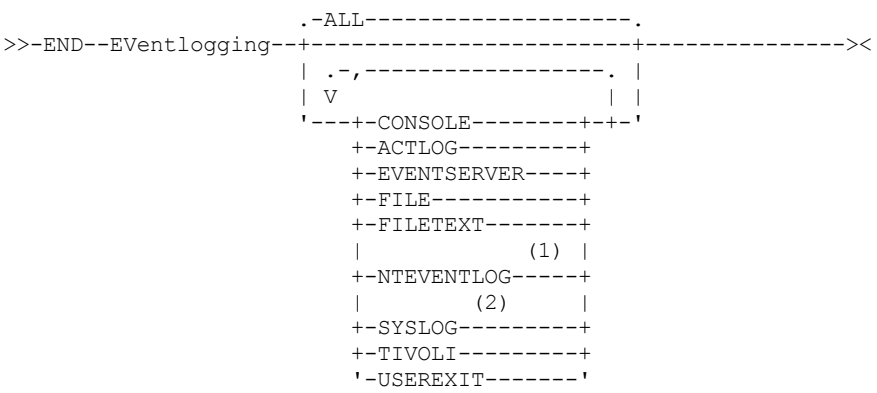
END EVENTLOGGING (Stop logging events)

Use this command to stop logging events to an active receiver.

Privilege class

To issue this command, you must have system privilege.

Syntax



Notes:

1. This parameter is only available for Windows operating system.
2. This parameter is only available for the Linux operating system.

Parameters

Specify a type of receiver. You can specify multiple receivers by separating them with commas and no intervening spaces. This is an optional parameter. The default is ALL. If you specify ALL or no receiver, logging ends for all receivers.

ALL
: Specifies all receivers.

CONSOLE
: Specifies the server console as a receiver.

ACTLOG
: Specifies the IBM Spectrum Protect™ activity log as a receiver. Logging can be stopped only for client events.

EVENTSERVER
: Specifies the event server as a receiver.

FILE
: Specifies a user file as a receiver. Each logged event is a record in the file and a person cannot read each logged event easily.

FILETEXT
: Specifies a user file as a receiver. Each logged event is a fixed-size, readable line.

Windows NTEVENTLOG
: Windows Specifies the Windows application log as a receiver.

Linux SYSLOG
: Linux Specifies the Linux system log as a receiver.

TIVOLI
: Specifies the Tivoli Management Environment (TME) as a receiver.

USEREXIT
: Specifies a user-written routine to which IBM Spectrum Protect writes information as a receiver.

Example: Stop logging events

End logging of events to the user exit.

```
end eventlogging userexit
```

Related commands

Table 1. Commands related to END EVENTLOGGING

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DISABLE EVENTS	Disables specific events for receivers.
ENABLE EVENTS	Enables specific events for receivers.
QUERY ENABLED	Displays enabled or disabled events for a specific receiver.
QUERY EVENTRULES	Displays information about rules for server and client events.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

EXPIRE INVENTORY (Manually start inventory expiration processing)

Use this command to manually start inventory expiration processing. The inventory expiration process removes client backup and archive file copies from server storage. Removal is based on policy specifications in the backup and archive copy groups of the management classes to which the files are bound.

When you have the disaster recovery manager function for your IBM Spectrum Protect™ server, the inventory expiration process also removes eligible virtual volumes that are used by the following processes:

- Database backups of type BACKUPFULL, BACKUPINCR, and DBSNAPSHOT. The SET DRMDBBACKUPEXPIREDAYS command controls when these volumes are eligible for expiration.
- Recovery plan files of type RPFILE and RPFSNAPSHOT. The SET DRMRPFEXPIREDAYS command controls when these volumes are eligible for expiration.

The inventory expiration process that runs during server initialization does not remove these virtual volumes.

Only one expiration process is allowed at any time, but this process can be distributed among a maximum of 40 threads. If an expiration process is running, you cannot start another process.

You can set up automatic expiration processing with the EXPINTERVAL server option. If you set the EXPINTERVAL option to 0, the server does not run expiration automatically, and you must issue the EXPIRE INVENTORY command to start expiration processing.

This command creates a background process that can be canceled with the CANCEL PROCESS command. To display information about background processes, use the QUERY PROCESS command.

If this command is applied to a WORM volume, the volume returns to being a scratch volume if it has remaining space in which data can be written. Data on WORM volumes, including deleted and expired data, cannot be overwritten. Therefore, data can be written only in space that does not contain current, deleted, or expired data. If a WORM volume does not have any space available in which data can be written, it remains private. To remove the volume from the library, you must use the CHECKOUT LIBVOLUME command.

Run the EXPIRE INVENTORY command to delete files from server storage if they were not deleted when you used client delete operations.

For more information about client delete operations, see Backup-archive client options and commands.

Privilege class

To issue this command, you must have system privilege.

Syntax

Parameters

Quiet
: Specifies whether the server suppresses detailed messages about policy changes during the expiration processing. This parameter is optional. The default is NO. Possible values are:

  No
  : Specifies that the server sends detailed informational messages.

  Yes
  : Specifies that the server sends only summary messages. The server issues messages about policy changes only when files are deleted and either the default management class or retention grace period for the domain was used to expire the files.

    You can also specify the EXPQUIET option in the server options file to automatically determine whether expiration processing is run with summary messages.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is NO. Possible values are:

  No
  : Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

    The server displays messages that are created from the background process either in the activity log or the server console, depending on where messages are logged.

  Yes
  : Specifies that the server processes this command in the foreground. You wait for the command to complete before you continue with other tasks. The server then displays the output messages to the administrative client when the command completes.
    Restriction: You cannot specify WAIT=YES from the server console.

SKipdirs
: Specifies whether the server skips directory type objects during the expiration processing. This parameter is optional. The default is NO. Possible values are:

  No
  : Specifies that the server expires files and directories that are based on the appropriate policy criteria.

Yes

Specifies that the server skips directory type backup and archive objects during expiration processing, even if the directories are eligible for expiration. By specifying YES, you prevent deletion of directories, and expiration processing can occur more quickly.
Attention: Do not use this option all of the time. With IBM Spectrum Protect Version 6.0 and later, you can run multiple threads (resources) for an expiration process. Also, if you specify YES often, the database grows as the directory objects accumulate, and the time that is spent for expiration increases. Run SKIPDIRS=NO periodically to expire the directories and reduce the size of the database.

Nodes

Specifies the name of the client nodes or node groups whose data is to be processed. To specify multiple node and node group names, separate the names with commas and no intervening spaces. Node names can contain wildcard characters, but node group names cannot. This parameter is optional.

You can specify NODES, EXCLUDENODES, DOMAIN, or any combination. If you specify more than one of these parameters, only those nodes that match the criteria for both NODES and DOMAIN and does not match the criteria for EXCLUDENODES command options are processed. If you do not specify NODES, EXCLUDENODES, or DOMAIN with a value, data for all nodes is processed.

EXCLUDENodes

Specifies the name of the client nodes or node groups whose data is not to be processed. To specify multiple node and node group names, separate the names with commas and no intervening spaces. Node names can contain wildcard characters, but node group names cannot. This parameter is optional.

You can specify NODES, EXCLUDENODES, DOMAIN, or any combination. If you specify more than one of these parameters, only those nodes that match the criteria for both NODES and DOMAIN and does not match the criteria for EXCLUDENODES command options are processed. If you do not specify NODES, EXCLUDENODES, or DOMAIN with a value, data for all nodes is processed.

Domain

Specifies that only data for client nodes that are assigned to the specified domain is to be processed. This parameter is optional. You can specify NODES, EXCLUDENODES, DOMAIN, or any combination. If you specify more than one of these parameters, only those nodes that match the criteria for both NODES and DOMAIN and does not match the criteria for EXCLUDENODES command options are processed. If you do not specify NODES, EXCLUDENODES, or DOMAIN with a value, data for all nodes is processed.

Type

Specifies the type of data to be processed. This parameter is optional. The default value is ALL. Possible values are:

ALl

Process all types of data that is eligible for expiration

Archive

Process only client archive data

Backup

Process only client backup data

Other

Process only items for disaster recovery manager functions, such as recovery plan files and obsolete database backups

REsource

Specifies the number of threads that can run in parallel. Specify a value in the range 1 - 40. This parameter is optional. The default is four.

Expiration runs as a single process, although the resources represent parallel work by the server within the single expiration process. Archive data for a node runs only on a single resource, but backup data can be spread across resources on a file space level. For example, if you specify `NODE=X,Y,Z` each with three file spaces and `RESOURCE=5`, then expiration processing for the three X, Y, and Z client nodes runs in parallel. At least one resource processes each node, and at least one node uses multiple resources for processing backup data across the multiple file spaces.

DUration

Specifies the maximum number of minutes for the expiration process to run. The process stops when the specified number of minutes pass or when all eligible expired objects are deleted, whichever comes first. Specify a value in the range 1 - 2880. This parameter is optional. If this parameter is not specified, the duration of the expiration process is not limited by time.

Example: Run inventory expiration processing for a specific time period

Run the expiration process for two hours.

```
expire inventory duration=120
```

Example: Run inventory expiration processing for backup data for two client nodes

Run inventory expiration processing for the backup data for two client nodes, CHARLIE and ROBBIE. Allow the server to run expiration processing until completed.

```
expire inventory nodes=charlie,robbie resource=2 type=backup
```

Example: Run inventory expiration processing for all client nodes except two nodes

Run inventory expiration processing for all client nodes except two nodes, CHARLIE and ROBBIE. Allow the server to run expiration processing until completed.

```
expire inventory excludenodes=charlie,robbie
```

Example: Run inventory expiration processing for all client nodes in a domain except one node

Run inventory expiration processing for all client nodes in a domain except one node, ROBBIE. Allow the server to run expiration processing until completed.

```
expire inventory domain=standard excludenodes=robbie
```

Related commands

Table 1. Commands related to EXPIRE INVENTORY

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.
CANCEL EXPIRATION	Cancels inventory expiration processing.
CANCEL PROCESS	Cancels a background server process.
QUERY PROCESS	Displays information about background processes.

EXPORT commands

Use the EXPORT commands to copy information from an IBM Spectrum Protect™ server to sequential removable media.

Important: For commands that export administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the EXPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

- EXPORT ADMIN (Export administrator information)
- EXPORT NODE (Export client node information)
- EXPORT POLICY (Export policy information)
- EXPORT SERVER (Export server information)

EXPORT ADMIN (Export administrator information)

Use this command to export administrator and authority definitions from a server. You can export the information to sequential media for later importing to another server, or you can export the information directly to another server for immediate import.

Important: For commands that export administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect™ server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already

synchronized by that server, you must update the password. After issuing the EXPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

IBM Spectrum Protect exports administrator information such as:

- Administrator name, password, and contact information
- Administrative privilege classes that are granted to the administrator
- Whether the administrator ID is locked from server access

You can use the QUERY ACTLOG command to view the status of the export operation. You can also view this information from the server console.

This command generates a background process that can be canceled with the CANCEL PROCESS command. If you export information to sequential media and the background process is canceled, the sequential media that is holding the exported data is incomplete, it must not be used for importing data. If a server-to-server export background process is canceled, a partial import might result. Evaluate any imported data on the target server to determine whether you want to keep or delete the imported data. Review the import messages for details. To display information about background processes, use the QUERY PROCESS command.

The following restrictions apply to the export function:

- Export operations from a later version and release to an earlier version and release is not supported.
- Export operations between servers that are at the same version and release but with different fix packs might fail. For example, you cannot export from a V7.1.3 server to a V7.1.1 or earlier server.
- Exported data from a server with retention protection enabled is not protected by retention when it is imported to another server.
- Export processing excludes nodes of type network-attached storage (NAS).
- Exporting data to a Centera device class or importing data from a Centera device class is not supported. However, files that are stored in Centera storage pools can be exported and files that must be imported can be stored on a Centera storage device.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

The EXPORT ADMIN command takes two forms: Export directly to another server on the network, or export to sequential media. The syntax and parameters for each form are defined separately.

Table 1. Commands related to EXPORT ADMIN

Command	Description
CANCEL PROCESS	Cancels a background server process.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT POLICY	Copies policy information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT ADMIN	Restores administrative information from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

- EXPORT ADMIN (Export administrator definitions to sequential media)
  You can export administrator and authority definitions from a server to sequential media for later importing to another server.
- EXPORT ADMIN (Export administrator information directly to another server)
  Use this command to export administrator and authority definitions directly to another server on the network. This results in an immediate import on the target server.

EXPORT ADMIN (Export administrator definitions to sequential media)

You can export administrator and authority definitions from a server to sequential media for later importing to another server.

Privilege class

To issue this command, you must have system privilege.

Syntax

Notes:

1. If PREVIEW=NO, a device class must be specified.
2. If PREVIEW=NO and SCRATCH=NO, one or more volumes must be specified.

Parameters

admin_name
: Specifies the administrators for which information is to be exported. This parameter is optional. The default is all administrators.

  Separate the items in the list by commas, with no intervening spaces. You can use wildcard characters to specify names.

Preview
: Specifies whether to preview the results of the export operation, without exporting information. You can use this parameter to preview how many bytes of data are transferred, and determine how many volumes are required. The following parameter values are supported:

  No

Specifies that the administrator information is to be exported. If you specify this value, you must specify a device class.

Yes

Specifies that the operation is previewed but not completed. Information is reported to the server console and the activity log. If you specify this value, you do not need to specify a device class.

This parameter is optional. The default value is NO.

DEVclass

Specifies the device class to which export data is to be written. This parameter is required if you specify PREVIEW=NO.

You cannot specify the DISK, NAS, or CENTERA device classes.

If all drives for the device class are busy when the export runs, IBM Spectrum Protect™ cancels lower priority operations to make a drive available.

Tip: You can export data to a storage pool on another server by specifying a device class whose device type is SERVER.

Scratch

Specifies whether scratch volumes can be used. The default value is YES. You can specify one of the following values:

Yes

Specifies that scratch volumes can be used for export. If you also specify a list of volumes, scratch volumes are used only if there is not enough space on the volumes specified.

No

Specifies that scratch volumes cannot be used for export. To determine how many volumes you might need, you can run the command specifying PREVIEW=YES.

VOLumenames

Specifies the volumes to be used to contain exported data. This parameter is optional, unless you specify SCRATCH=NO and PREVIEW=NO. If you do not specify a volume name, scratch volumes are used.

You can specify one of the following values:

volume_name

Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

FILE:file_name

Specifies the name of a file that contains a list of volumes. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when specifying volumes associated with the following device types:

For this device	**Specify**
Tape	1-6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: AIX Linux /imdata/mt1. Windows d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1-6 alphanumeric characters.
SERVER	1-250 alphanumeric characters.

USEDVolumelist

Specifies the file where a list of volumes used in the export operation are stored. This parameter is optional.

This file can be used in the import operation. This file contains comment lines with the date and time the export was done, and the command issued to create the export.

Attention: If you specify an existing file, the file is overwritten.

ENCryptionstrength

Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

AES

Specifies the Advanced Encryption Standard.

DES

Specifies the Data Encryption Standard.

Example: Export administrator definitions to tape volumes

From the server, export the information for all defined administrators to tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class. The number and types of objects that are exported are reported to the system console and in the activity log. Issue the command:

```
export admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Example: Export administrator definitions to tape volumes listed in a file

From the server, export the information for all defined administrators to tape volumes that are listed in the following file:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

This file contains the following lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that these tape volumes be used by a device that is assigned to the MENU1 device class. Issue the command:
AIX Linux

```
export admin devclass=menu1 volumenames=file:tapevol
```

Windows

```
export admin devclass=menu1 volumenames=file:tapevol.data
```

The number and types of objects that are exported are reported to the system console and in the activity log.

EXPORT ADMIN (Export administrator information directly to another server)

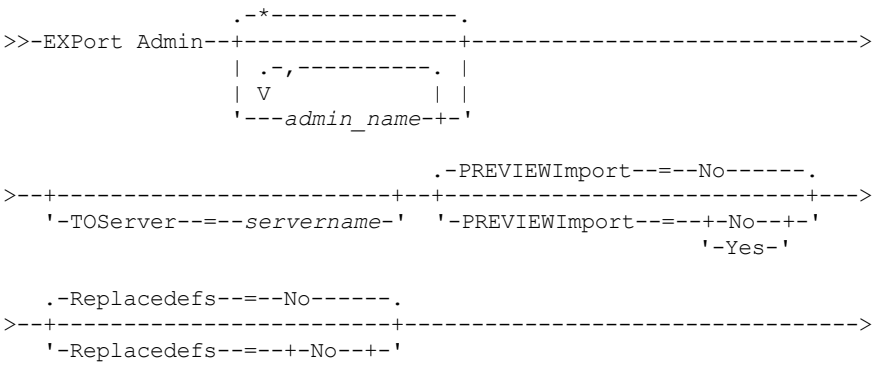
Use this command to export administrator and authority definitions directly to another server on the network. This results in an immediate import on the target server.

You can issue a QUERY PROCESS command from the target server to monitor the progress of the import operation. See EXPORT ADMIN (Export administrator information) for a list of restrictions that apply to the export function.

Privilege class

To issue this command, you must have system privilege.

Syntax



```
                    '-Yes-'

   .-ENCryptionstrength--=--AES-----.
>--+-------------------------------+-------------------------><
   '-ENCryptionstrength--=--+-AES-+-'
                            '-DES-'
```

Parameters

admin_name
: Specifies the administrators for which information is to be exported. This parameter is optional. The default is all administrators.

  Separate the items in the list by commas, with no intervening spaces. You can use wildcard characters to specify names.

TOServer
: Specifies the name of a server to which the export data is sent directly over the network for immediate import.
  Important: The target server must be defined on the originating server with the DEFINE SERVER command. The administrator that issues the export command must be defined with the same administrator name and password and have system authority on the target server.

  When you specify TOSERVER, you cannot specify the DEVCLASS, VOLUMENAMES, and SCRATCH, USEDVOLUMELIST, and PREVIEW parameters.

PREVIEWImport
: Specifies whether to view how much data is transferred, without actually moving any data. This information can be used to determine how much storage pool space is required on the target server. The default is NO.
  Valid values are:

  Yes
  : Specifies that you want to preview the results of the import operation on the target server, without importing the data. Information is reported to the server console and the activity log.

  No
  : Specifies that you want the data to be imported on the target server without previewing the results.

Replacedefs
: Specifies whether to replace definitions (not file data) on the server. The default is NO.

  Valid values are:

  Yes
  : Specifies that definitions are replaced on the server if definitions having the same name as those being imported exist on the target server.

  No
  : Specifies that imported definitions are skipped if their names conflict with definitions that are already defined on the target server.

ENCryptionstrength
: Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

  AES
  : Specifies the Advanced Encryption Standard.

  DES
  : Specifies the Data Encryption Standard.

Example: Export administrator definitions to a target server

Export all the administrator definitions to the target server defined as OTHERSERVER. Preview the import operations on the target server. Issue the command:

```
export admin * toserver=otherserver previewimport=yes
```

From the target server, OTHERSERVER, you can view the import operations by issuing the command:

EXPORT NODE (Export client node information)

Use this command to export client node definitions or file data to sequential media or directly to another server for immediate import.

Important: For commands that export administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect™ server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the EXPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.
The following information is included in each client node definition:

- User ID, password, and contact information.
- Name of the client's assigned policy domain.
- File compression status.
- Whether the user has the authority to delete backed-up or archived files from server storage.
- Whether the client node ID is locked from server access.

Optionally, you can also export the following items:

- File space definitions.
- Backed-up, archived, and files that were migrated by an IBM Spectrum Protect for Space Management client.
- Access authorization information that pertains to the file spaces exported.
- Archive data that is in deletion hold status (the hold status is preserved). When the archive data is imported, it remains in deletion hold.

If you use an LDAP directory server to authenticate passwords, any servers that you export to must be configured for LDAP passwords. Node data that is exported from a node that authenticates with an LDAP directory server is inaccessible if the target server is not properly configured. If your target server is not configured, exported data from an LDAP node can still be exported. But the target server must be configured to use LDAP, to access the data.

The following restrictions apply to the export function:

- Export operations from a later version and release to an earlier version and release is not supported.
- Export operations between servers that are at the same version and release but with different fix packs might fail. For example, you cannot export from a V7.1.3 server to a V7.1.1 or earlier server.
- Exported data from a server with retention protection enabled is not protected by retention when it is imported to another server.
- Export processing excludes nodes of type network-attached storage (NAS).
- Exporting data to a Centera device class or importing data from a Centera device class is not supported. However, files that are stored in Centera storage pools can be exported and files that must be imported can be stored on a Centera storage device.

- The EXPORT NODE and EXPORT SERVER commands do not export data from a shred pool unless you explicitly allow it by setting the ALLOWSHREDDABLE parameter to the YES value. If this value is specified, and the exported data includes data from shred pools, that data cannot be shredded. A warning is not issued if the export operation includes data from shred pools.

- Incrementally exporting or importing the following types of client data to another IBM Spectrum Protect server is not supported:
  - VMware backups where full plus incremental backups need to be periodically, incrementally transferred to another server
  - Backups groups where full plus differential backups must be periodically, incrementally transferred to another server
  - Windows System State data that is periodically, incrementally transferred to another server

  Full export or import of this data to a new file system on the target is supported by exporting the entire file space that contains the data. The export must not use the FILEDATA=ALLACTIVE, FROMDATE, TODATE, or MERGEFILESPACES parameters.

  Using node replication to incrementally transfer this type of client data between two servers is optimal.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

The EXPORT NODE command generates a background process that can be canceled with the CANCEL PROCESS command. If you are exporting node information to sequential media and the background process is canceled, the sequential media that is holding the exported data is incomplete, it must not be used to import data. If a server-to-server export background process is canceled, a partial import might result. Evaluate any imported data on the target server to determine whether you want to keep or delete the imported data. Review the import messages for details. To display information about background processes, issue the QUERY PROCESS command.

To display information about any running and suspended server-to-server export operations, issue the QUERY EXPORT command. The QUERY EXPORT command displays information only for exports that are, or can be, suspended. Export operations that can be suspended, and then restarted, are those server-to-server exports whose FILEDATA has a value other than NONE. You can issue the QUERY ACTLOG command to view the status of the export operation.

Because of unpredictable results, do not run expiration, migration, backup, or archive when you are issuing the EXPORT NODE command.

For a server that has clients with support for Unicode, you can get the server to convert the file space name that you enter, or use one of the following parameters:

- FSID
- UNIFILESPACE

The EXPORT NODE command takes two forms: export directly to another server on the network, or export to sequential media. The syntax and parameters for each form are defined separately.

Table 1. Commands related to EXPORT NODE

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.
EXPORT ADMIN	Copies administrative information to external media or directly to another server.
EXPORT POLICY	Copies policy information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT NODE	Restores client node information from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
QUERY PROCESS	Displays information about background processes.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

- EXPORT NODE (Export node definitions to sequential media)
  You can export node definitions or file data from a server to sequential media for later importing to another server.
- EXPORT NODE (Export node definitions or file data directly to another server)
  Use this command to export client node definitions or file data directly to another server for immediate import.

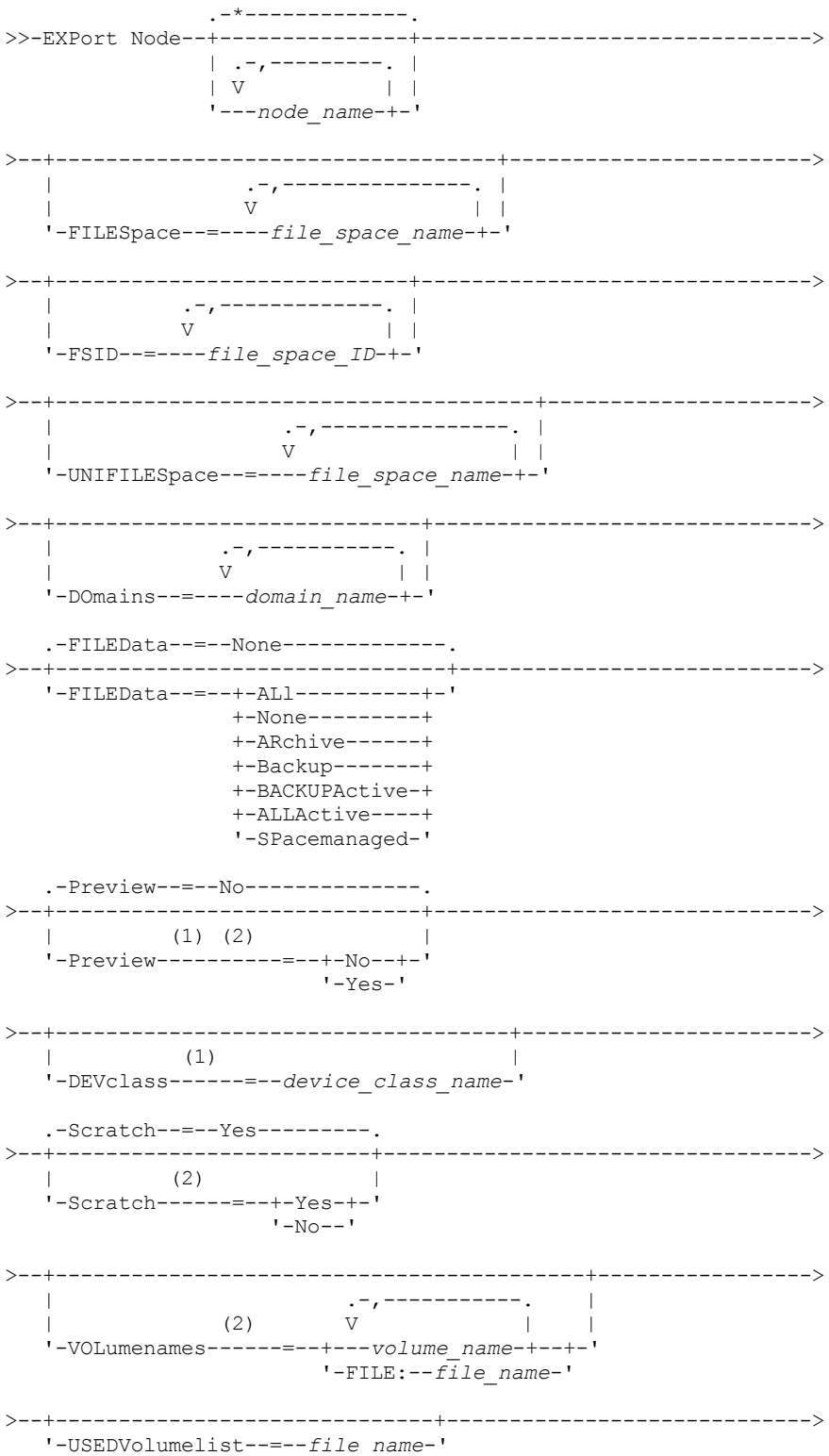
EXPORT NODE (Export node definitions to sequential media)

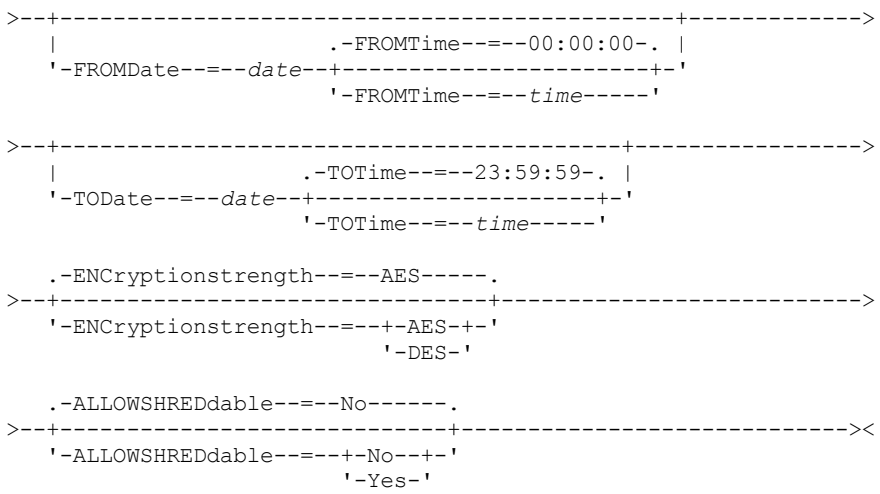
You can export node definitions or file data from a server to sequential media for later importing to another server.

Privilege class

To issue this command, you must have system privilege.

Syntax





Notes:

1. If PREVIEW=NO, a device class must be specified.
2. If PREVIEW=NO and SCRATCH=NO, one or more volumes must be specified.

Parameters

node_name
: Specifies the client node names for which information is to be exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. For each node entered, all file spaces in the file space, FSID, and Unicode enabled lists are searched.
Restriction: If you use wildcard characters to specify a pattern for node names, the server does not report the node names or patterns that do not match any entries in the database. Check the summary statistics in the activity log to verify that the server exported all intended nodes.

FILESpace
: Specifies the file spaces for which data is to be exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify a name.
Restriction: If a file space is specified, Unicode enabled file spaces are not exported.

FSID
: Specifies the file spaces by using their file space IDs (FSIDs). The server uses the FSIDs to find the file spaces to export. To find the FSID for a file space, use the QUERY FILESPACE command. Separate multiple file space IDs with commas and no intervening spaces. This parameter is optional.

UNIFILESpace
: Specifies the file spaces that are known to the server as Unicode enabled. The server converts the names that you enter from the server code page to the UTF-8 code page to find the file spaces to export. The success of the conversion depends on the actual characters in the name and the server's code page. Separate multiple names with commas and no intervening spaces. A wildcard character can be used to specify a name. This parameter is optional.

DOmains
: Specifies the policy domains from which nodes are to be exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. If you specify domains, a node is exported only if it belongs to one of the specified domains. You can use wildcard characters to specify a name.

FILEData
: Specifies the type of files that are to be exported for all nodes that are being exported to the server. This parameter is optional. The default value is NONE.
Note: If you are exporting a node that has group data, data that is not a part of the target objects might be exported. An example of group data is virtual machine data or system state backup data. For example, if FILEDATA=BACKUPACTIVE when the FROMDATE or TODATE parameters are specified, it is possible to include inactive backup data. The incremental backup processing for the data can cause extra files that do not meet the filtering criteria to be exported.

  If you are exporting to sequential media: the device class that is used by the file data is determined by the device class for the storage pool. If it is the same device class that is specified in this command, two drives are needed to export node information. The mount limit for the device class must be at least 2.

  Important: If client nodes registered as TYPE=SERVER are being exported, specify ALL, ARCHIVE, or ALLACTIVE.

The following descriptions mention *active* and *inactive* backup file versions. An active backup file version is the most recent backup version for a file that still exists on the client workstation. All other backup file versions are called inactive copies. This parameter supports the following values:

ALl
: The server exports all backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect™ for Space Management client.

None
: The server does not export files, only node definitions.

ARchive
: The server exports only archived files.

Backup
: The server exports only backup versions, whether active or inactive.

BACKUPActive
: The server exports only active backup versions. These active backup versions are the active versions in the IBM Spectrum Protect database at the time that the EXPORT command is issued.

ALLActive
: The server exports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client. The active backup versions are the active versions in the IBM Spectrum Protect database at the time that the EXPORT command is issued.

SPacemanaged
: The server exports only files that were migrated by an IBM Spectrum Protect for Space Management client.

Preview
: Specifies whether to preview the results of the export operation, without exporting information. You can use this parameter to preview how many bytes of data would be transferred so that you can determine how many volumes are required. This parameter supports the following values:

  No
  : Specifies that the node information is to be exported. If you specify this value, you must also specify a device class.

  Yes
  : Specifies that the operation is previewed but not completed. Information is reported to the server console and the activity log. If you specify this value, you do not need to specify a device class.

  This parameter is optional. The default value is NO.

DEVclass
: Specifies the device class to which export data is to be written. This parameter is required if you specify PREVIEW=NO.

  You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the export runs, IBM Spectrum Protect cancels lower priority operations to make a drive available.

  Tip: You can export data to a storage pool on another server by specifying a device class whose device type is SERVER.

Scratch
: Specifies whether scratch volumes can be used. The default value is YES. You can specify one of the following values:

  Yes
  : Specifies that scratch volumes can be used for export. If you also specify a list of volumes, scratch volumes are used only if there is not enough space on the volumes specified.

  No
  : Specifies that scratch volumes cannot be used for export. To determine how many volumes you might need, you can run the command specifying PREVIEW=YES.

VOLumenames
: Specifies the volumes to be used to contain exported data. This parameter is optional, unless you specify SCRATCH=NO and PREVIEW=NO. If you do not specify a volume name, scratch volumes are used.

  You can specify one of the following values:

  volume_name
  : Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

  FILE:file_name

Specifies the name of a file that contains a list of volumes. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when specifying volumes associated with the following device types:

For this device	Specify
Tape	1-6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: AIX Linux /imdata/mt1. Windows d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1-6 alphanumeric characters.
SERVER	1-250 alphanumeric characters.

USEDVolumelist

Specifies the file where a list of volumes used in the export operation are stored. This parameter is optional.

This file can be used in the import operation. This file contains comment lines with the date and time the export was done, and the command issued to create the export.

Attention: If you specify an existing file, the file is overwritten.

FROMDate

Specifies the earliest date for which files to be exported were stored on the server. Files that were stored on the server earlier than the specified date are not exported. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. IBM Spectrum Protect ignores the FROMDATE parameter when the FILEDATA parameter is set to NONE.

Directory processing: The FROMDATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.

Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. Group data on the node is, for example, virtual machine data or system state backup data. This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.

Use one of the following values to specify the date:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

If this parameter is not specified, IBM Spectrum Protect exports all objects stored before the TODATE parameter and as qualified by the FILEDATA parameter. If no TODATE parameter is specified, then all data as qualified by the FILEDATA parameter is exported.

When a server-to-server export operation uses a relative FROMDATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the FROMDATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

TODate

Specifies the latest date for files to be exported from the server. Files stored on the server on a date later than the TODATE value are not exported. TODATE only applies to client file data and does not affect other information that is being exported, such as policy.

- IBM Spectrum Protect ignores the TODATE parameter when the FILEDATA parameter is set to NONE.
- If a TODATE parameter is specified without a TOTIME parameter, the server exports all objects that are inserted on or before the day specified by the TODATE parameter.
- If you specified the FROMDATE parameter, the value of TODATE must be later than or equal to the FROMDATE value. If the TODATE and FROMDATE are equal, then the TOTIME parameter must be later that the FROMTIME parameter.
- The TODATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.

Important: If you have group data on the node that you are exporting, data that was backed up after the TODATE or TOTIME parameters can be exported. An example of group data is virtual machine data or system state backup data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.

Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	10/15/2006
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –3 **or** –3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

When a server-to-server export operation uses a relative TODATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the TODATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted 10 days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

FROMTime

Specifies the earliest time for which objects to be exported were stored on the server. When you specify FROMTIME, you must also use the FROMDATE parameter. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. Objects that were stored on the server before the specified time and date are not exported. IBM Spectrum Protect ignores the FROMTIME parameter when the FILEDATA parameter is set to NONE.

Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. An example of group data on the node is virtual machine data or system state backup data, This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported so that there is a consistent image for the backup data.

The default value for this parameter when used with the FROMDATE parameter is midnight (00:00:00).

Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified. The FROMTIME+ can only be used with a FROMDATE before today.	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with FROMTIME=NOW+02:00 or FROMTIME=+02:00, the export operation only contains files that were put on the server after 7:00 on the FROMDATE that you specify.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW -02:00 **or** -02:00. If you issue this command at 5:00 with FROMTIME=NOW-02:00 or FROMTIME=-2:00, the export includes files that were put on the server after 3:00.

TOTime

Specifies the latest time that objects to be exported were stored on the server. You must specify the TODATE parameter in order to use the TOTIME parameter. TOTIME only applies to client file data and does not affect other information that is being exported, such as policy. IBM Spectrum Protect ignores the TOTIME parameter if the FILEDATA parameter is set to NONE.

The default value for this parameter, when used with the TODATE parameter, is midnight minus one second (23:59:59).

Important: The value of the TOTIME and TODATE parameters must be later than the FROMDATE and the FROMTIME value.
Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW+HH:MM **or**+HH:MM	The current time plus hours and minutes specified.	NOW+02:00 **or** +02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW+02:00, the export includes files that were stored from 01:00 until 07:00.
NOW-HH:MM **or**-HH:MM	The current time minus hours and minutes specified.	NOW-02:00 **or** -02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW-02:00, the export includes files that were stored from 01:00 until 03:00.

ENCryptionstrength

Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

AES
: Specifies the Advanced Encryption Standard.

DES
: Specifies the Data Encryption Standard.

ALLOWSHREDdable

Specifies whether data from a storage pool that enforces shredding is exported. This parameter supports the following values:

No
: Specifies that data is not exported from a storage pool that enforces shredding.

Yes
: Specifies that data can be exported from a storage pool that enforces shredding. The data on the export media is not shredded.

This parameter is optional. The default value is NO.

Example: Export client node information to specific tape volumes

From the server, export client node information to tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be used by a device that is assigned to the MENU1 device class.

```
export node devclass=menu1 volumenames=tape01,tape02,tape03
```

Example: Export client node information by using the FSID

From the server, use the FSID to export active backup versions of file data for client node JOE to tape volume TAPE01. To determine the FSID, first issue a QUERY FILESPACE command.

1. To determine the FSID, issue a QUERY FILESPACE command.

   ```
   query filespace joe
   ```

   ```
   Node Name Filespace  FSID Platform Filespace    Is     Capacity   Pct
             Name                     Type      Filespace    (MB)   Util
                                                 Unicode?
   --------- ---------- ---- -------  ---------  --------- -------- ----
   JOE       \\joe\c$      1  WinNT    NTFS         Yes     2,502.3  75.2
   JOE       \\joe\d$      2  WinNT    NTFS         Yes     6,173.4  59.6
   ```

2. Export the active backup versions of file data and specify that the tape volume is used by a device that is assigned to the MENU1 device class.

   ```
   export node joe fsid=1,2 filedata=backupactive devclass=menu1
   volumenames=tape01
   ```

Example: Export client node information to tape volumes listed in a file

From the server, export client node information to tape volumes that are listed in the following file:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

The file contains the following lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that the tape volumes be used by a device that is assigned to the MENU1 device class. Issue the following command:
AIX Linux

```
export node devclass=menu1 volumenames=file:tapevol
```

Windows

```
export node devclass=menu1 volumenames=file:tapevol.data
```

EXPORT NODE (Export node definitions or file data directly to another server)

Use this command to export client node definitions or file data directly to another server for immediate import.

Important: You cannot export nodes of type NAS. Export processing excludes these nodes.

You can suspend and restart a server-to-server export operation that has a FILEDATA value other than NONE. The server saves the state and status of the export operation so that it can be restarted from the point at which the operation failed or was suspended. The export operation can be restarted later by issuing the RESTART EXPORT command.

Important: An export operation is suspended when any of the following conditions are detected:

- A SUSPEND EXPORT command is issued for the running export operation
- Segment preemption - the file that is being read for export is deleted by some other process
- Communication errors on a server-to-server export
- No available mount points
- Necessary volumes are unavailable
- I/O errors encountered

Issue the QUERY EXPORT command to display information on any running and suspended export operations.

The export operation cannot be restarted if the export operation fails before transmitting the eligible node and file space definitions to the target server. You must reenter the command to begin a new export operation.

You can issue a QUERY PROCESS command from the target server to monitor the progress of the import operation. Issue the QUERY EXPORT command to list all restartable server-to-server export operations. See EXPORT ADMIN (Export administrator information) for a list of restrictions that apply to the export function.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                .-*---------.
>>-EXPort Node--+-----------+-------------------------------------->
                '-node_name-'

>--+-------------------------------+--------------------------->
   '-FILESpace--=--file_space_name-'

>--+-----------------------+----------------------------------->
   '-FSID--=--file_space_ID-'

>--+---------------------------------+------------------------>
   '-UNIFILESpace--=--file_space_name-'

>--+-------------------------+----------------------------------->
   '-DOmains--=--domain_name-'

   .-FILEData--=--None-------------.
>--+-------------------------------+--------------------------->
   '-FILEData--=--+-ALl----------+-'
                  +-None---------+
                  +-ARchive------+
                  +-Backup-------+
                  +-BACKUPActive-+
                  +-ALLActive----+
                  '-SPacemanaged-'

>--+-----------------------------------------------+------------>
   |                    .-FROMTime--=--00:00:00-. |
   '-FROMDate--=--date--+------------------------+-'
                        '-FROMTime--=--time-----'

>--+-----------------------------------------+----------------->
   |                   .-TOTime--=--23:59:59-. |
   '-TODate--=--date--+---------------------+-'
                      '-TOTime--=--time-----'

>--+-------------------------------------+------------------->
   '-EXPORTIDentifier--=--export_identifier-'
```

```
                                .-PREVIEWImport--=--No------.
>--+-------------------------+--+---------------------------+--->
   '-TOServer--=--servername-'  '-PREVIEWImport--=--+-No--+-'
                                                   '-Yes-'

   .-MERGEfilespaces--=--No------.
>--+-----------------------------+------------------------------>
   '-MERGEfilespaces--=--+-No--+-'
                         '-Yes-'

   .-Replacedefs--=--No------.
>--+-------------------------+-------------------------------->
   '-Replacedefs--=--+-No--+-'
                     '-Yes-'

   .-PROXynodeassoc--=--No------.
>--+----------------------------+------------------------------>
   '-PROXynodeassoc--=--+-No--+-'
                        '-Yes-'

   .-ENCryptionstrength--=--AES-----.
>--+--------------------------------+--------------------------->
   '-ENCryptionstrength--=--+-AES-+-'
                            '-DES-'

   .-ALLOWSHREDdable--=--No------.
>--+-----------------------------+------------------------------><
   '-ALLOWSHREDdable--=--+-No--+-'
                         '-Yes-'
```

Parameters

node_name
: Specifies the client node names for which information is to be exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. For each node entered, all file spaces in the file space, FSID, and Unicode enabled lists are searched.
Restriction: If you specify a list of node names or node patterns, the server does not report the node names or node patterns that do not match any of the entries in the database. Check the summary statistics in the activity log to verify that the server exported all intended nodes.

FILESpace
: Specifies the file spaces for which data is to be exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify a name.
Restriction: If a file space is specified, no Unicode enabled file spaces are exported.

FSID
: Specifies the file spaces by using their file space IDs (FSIDs). The server uses the FSIDs to find the file spaces to export. To find the FSID for a file space, use the QUERY FILESPACE command. Separate multiple file space IDs with commas and no intervening spaces. This parameter is optional.

UNIFILESpace
: Specifies the file spaces that are known to the server to be Unicode enabled. The server converts the names that you enter from the server code page to the UTF-8 code page to find the file spaces to export. The success of the conversion depends on the actual characters in the name and the server's code page. Separate multiple names with commas and no intervening spaces. A wildcard character can be used to specify a name. This parameter is optional.

DOmains
: Specifies the policy domains from which nodes are exported. This parameter is optional. Separate multiple names with commas and no intervening spaces. If you specify domains, IBM Spectrum Protect™ exports a node only if it belongs to one of the specified domains. You can use wildcard characters to specify a name.

FILEData
: Specifies the type of files to export for all nodes. This parameter is optional. The default value is NONE.
Note: If you are exporting a node that has group data, data that is not a part of the target objects might be exported. An example of group data is virtual machine data or system state backup data. For example, if FILEDATA=BACKUPACTIVE when the FROMDATE or TODATE parameters are specified, it is possible to include inactive backup data. The incremental backup processing for the data can cause extra files that do not meet the filtering criteria to be exported.

  If you are exporting to sequential media, the device class that is used by the file data is determined by the device class for the storage pool. If it is the same device class that is specified in this command, IBM Spectrum Protect requires two drives to export node information. The mount limit for the device class must be at least 2.

Important: If you export client nodes that are registered as TYPE=SERVER, specify ALL, ARCHIVE, or ALLACTIVE.
The following descriptions mention *active* and *inactive* backup file versions. An active backup file version is the most recent backup version for a file that still exists on the client workstation. All other backup file versions are called inactive copies.
The values are as follows:

ALl
: The server exports all backup versions of files, all archived files, and all files that are migrated by an IBM Spectrum Protect for Space Management client.

None
: The server does not export files, only node definitions.

ARchive
: The server exports only archived files.

Backup
: The server exports only backup versions, whether they are active or inactive.

BACKUPActive
: The server exports only active backup versions. These active backup versions are the active versions in the IBM Spectrum Protect database at the time that the EXPORT command is issued.

ALLActive
: The server exports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client. The active backup versions are the active versions in the IBM Spectrum Protect database at the time that the EXPORT command is issued.

SPacemanaged
: The server exports only files that were migrated by an IBM Spectrum Protect for Space Management client.

FROMDate
: Specifies the earliest date for which files to be exported were stored on the server. Files that were stored on the server earlier than the specified date are not exported. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. IBM Spectrum Protect ignores the FROMDATE parameter when the FILEDATA parameter is set to NONE.
Directory processing: The FROMDATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.
Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. Group data on the node is, for example, virtual machine data or system state backup data. This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.
Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

If this parameter is not specified, IBM Spectrum Protect exports all objects stored before the TODATE parameter and as qualified by the FILEDATA parameter. If no TODATE parameter is specified, then all data as qualified by the FILEDATA parameter is exported.

When a server-to-server export operation uses a relative FROMDATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the FROMDATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

TODate

Specifies the latest date for files to be exported from the server. Files that are stored on the server on a date later than the TODATE value are not exported. TODATE only applies to client file data and does not affect other information that is being exported, such as policy.

- IBM Spectrum Protect ignores the TODATE parameter when the FILEDATA parameter is set to NONE.
- If a TODATE parameter is specified without a TOTIME parameter, the server exports all objects that are inserted on or before the day specified by the TODATE parameter.
- If you specified the FROMDATE parameter, the value of TODATE must be later than or equal to the FROMDATE value. If the TODATE and FROMDATE are equal, then the TOTIME parameter must be later that the FROMTIME parameter.
- The TODATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.

Important: If you have group data on the node that you are exporting, data that was backed up after the TODATE or TOTIME parameters can be exported. An example of group data is virtual machine data or system state backup data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.

Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	10/15/2006
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –3 **or** –3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

When a server-to-server export operation uses a relative TODATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the TODATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted 10 days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

FROMTime

Specifies the earliest time for which objects to be exported were stored on the server. When you specify FROMTIME, you must also use the FROMDATE parameter. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. Objects that were stored on the server before the specified time and date are not exported. IBM Spectrum Protect ignores the FROMTIME parameter when the FILEDATA parameter is set to NONE.

Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. An example of group data on the node is virtual machine data or system state backup data, This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported so that there is a consistent image for the backup data.

The default value for this parameter when used with the FROMDATE parameter is midnight (00:00:00).

Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified. The FROMTIME+ can only be used with a FROMDATE before today.	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with FROMTIME=NOW+02:00 or FROMTIME=+02:00, the export operation only contains files that were put on the server after 7:00 on the FROMDATE that you specify.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW -02:00 **or** -02:00. If you issue this command at 5:00 with FROMTIME=NOW-02:00 or FROMTIME=-2:00, the export includes files that were put on the server after 3:00.

TOTime

Specifies the latest time that objects to be exported were stored on the server. You must specify the TODATE parameter in order to use the TOTIME parameter. TOTIME only applies to client file data and does not affect other information that is being exported, such as policy. IBM Spectrum Protect ignores the TOTIME parameter if the FILEDATA parameter is set to NONE.

The default value for this parameter, when used with the TODATE parameter, is midnight minus one second (23:59:59).

Important: The value of the TOTIME and TODATE parameters must be later than the FROMDATE and the FROMTIME value.
Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW+HH:MM **or**+HH:MM	The current time plus hours and minutes specified.	NOW+02:00 **or** +02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW+02:00, the export includes files that were stored from 01:00 until 07:00.
NOW-HH:MM **or**-HH:MM	The current time minus hours and minutes specified.	NOW-02:00 **or** -02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW-02:00, the export includes files that were stored from 01:00 until 03:00.

TOServer

Specifies the name of a server to which the export data is sent directly over the network for immediate import.
Important: The target server must be defined on the originating server with the DEFINE SERVER command. The administrator that issues the export command must be defined with the same administrator name and password and have system authority on the target server.

When you specify TOSERVER, you cannot specify the DEVCLASS, VOLUMENAMES, and SCRATCH, USEDVOLUMELIST, and PREVIEW parameters.

PREVIEWImport

Specifies whether to view how much data is transferred, without actually moving any data. This information can be used to determine how much storage pool space is required on the target server. The default is NO.
Valid values are:

Yes
: Specifies that you want to preview the results of the import operation on the target server, without importing the data. Information is reported to the server console and the activity log.

No
: Specifies that you want the data to be imported on the target server without previewing the results.

MERGEfilespaces
: Specifies whether IBM Spectrum Protect merges client files into existing file spaces on the target server (if they exist), or if IBM Spectrum Protect generates new file space names. The default is NO.

Valid values are:

Yes
: Specifies that imported data on the target server is merged with the existing file space, if a file space with the same name exists on the target server.

No
: Specifies that IBM Spectrum Protect generates a new file space name for imported data on the target server if file spaces with the same name exists.

Replacedefs
: Specifies whether to replace definitions (not file data) on the server. The default is NO.

Valid values are:

Yes
: Specifies that definitions are replaced on the server if definitions having the same name as those being imported exist on the target server.

No
: Specifies that imported definitions are skipped if their names conflict with definitions that are already defined on the target server.

PROXynodeassoc
: Specifies if proxy node associations are exported. This parameter is optional. The default value is NO.

ENCryptionstrength
: Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

AES
: Specifies the Advanced Encryption Standard.

DES
: Specifies the Data Encryption Standard.

ALLOWSHREDdable
: Specifies whether data from a storage pool that enforces shredding is exported. This parameter is optional. The default value is NO. Possible values are:

No
: Specifies that the server does not export data from a storage pool that enforces shredding.

Yes
: Specifies that the server does export from a storage pool that enforces shredding. The data on the export media is not shredded.

Restriction: After an export operation finishes identifying files for export, any changes to the storage pool ALLOWSHREDABLE value is ignored. An export operation that is suspended retains the original ALLOWSHREDABLE value throughout the operation. You might want to consider canceling your export operation if changes to the storage pool ALLOWSHREDABLE value jeopardize the operation. You can reissue the export command after any needed cleanup.

EXPORTIDentifier
: This optional parameter specifies the name that you select to identify this export operation. If you do not specify an identifier name, the server generates one for you. The export identifier name cannot be more than 64 characters, cannot

contain wildcard characters, and is not case-sensitive. You can use the identifier name to reference export operations in the QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT, or CANCEL EXPORT commands.
Restriction: You must specify the TOSERVER parameter if you are specifying the EXPORTIDENTIFIER parameter. EXPORTIDENTIFIER is ignored if FILEDATA=NONE.

Example: Export client node information and all client files

To export client node information and all client files for NODE1 directly to SERVERB, issue the following command:

```
export node node1 filedata=all toserver=serverb
```

Example: Export client node information and all client files for a specific date range

To export client node information and all client files for NODE1 directly to SERVERB between February 1, 2009 and today.

```
export node node1 filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

Example: Export client node information and all client files for a specific date and time range

To export client node information and all client files for NODE1 directly to SERVERB from 8:00 AM on February 1, 2009 until today at 8:00 AM, issue the following command:

```
export node node1 filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

Example: Export client node information and all client files for the past three days

To export client node information and all client files for NODE1 directly to SERVERB for the past three days, issue the following command:

```
export node node1 filedata=all toserver=serverb
fromdate=today -3
```

EXPORT POLICY (Export policy information)

Use this command to export policy information from an IBM Spectrum Protect™ server to sequential media or directly to another server for immediate import. When a policy is exported by using the EXPORT POLICY command, the active data pool information in the domain is not exported.

The server exports policy information, such as:

- Policy domain definitions
- Policy set definitions, including the active policy set
- Management class definitions, including the default management class
- Backup copy group and archive copy group definitions
- Schedule definitions for each policy domain
- Client node associations, if the client node exists on the target server

You can use the QUERY ACTLOG command to view the status of the export operation. You can also view this information from the server console.

This command generates a background process that can be canceled with the CANCEL PROCESS command. If you export policy information to sequential media and the background process is canceled, the sequential media that is holding the exported data is incomplete and must not be used to import data. If a server-to-server export background process is canceled, a partial import might result. Evaluate any imported data on the target server to determine whether you want to keep or delete the imported data. Review the import messages for details. To display information about background processes, use the QUERY PROCESS command.

The following restrictions apply to the export function:

- Export operations from a later version and release to an earlier version and release is not supported.
- Export operations between servers that are at the same version and release but with different fix packs might fail. For example, you cannot export from a V7.1.3 server to a V7.1.1 or earlier server.

- Exported data from a server with retention protection enabled is not protected by retention when it is imported to another server.
- Export processing excludes nodes of type network-attached storage (NAS).
- Exporting data to a Centera device class or importing data from a Centera device class is not supported. However, files that are stored in Centera storage pools can be exported and files that must be imported can be stored on a Centera storage device.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

The EXPORT POLICY command takes two forms: Export directly to another server on the network, or export to sequential media. The syntax and parameters for each form are defined separately.

Table 1. Commands related to EXPORT POLICY

Command	Description
CANCEL PROCESS	Cancels a background server process.
EXPORT ADMIN	Copies administrative information to external media or directly to another server.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT POLICY	Restores policy information from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

- EXPORT POLICY (Export policy information to sequential media)
  Use this command to export policy information from an IBM Spectrum Protect server to sequential media for later import to another server.
- EXPORT POLICY (Export a policy directly to another server)
  Use this command to export policy information directly to another server on the network. This results in an immediate import on the target server.

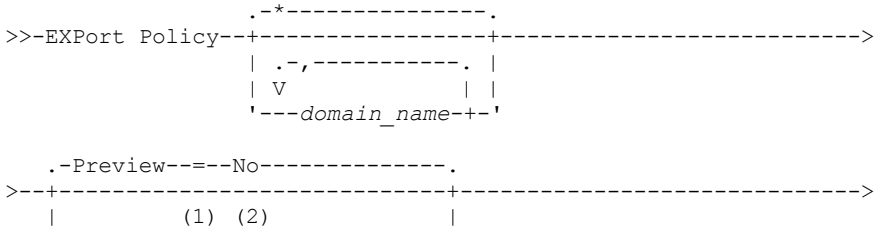
EXPORT POLICY (Export policy information to sequential media)

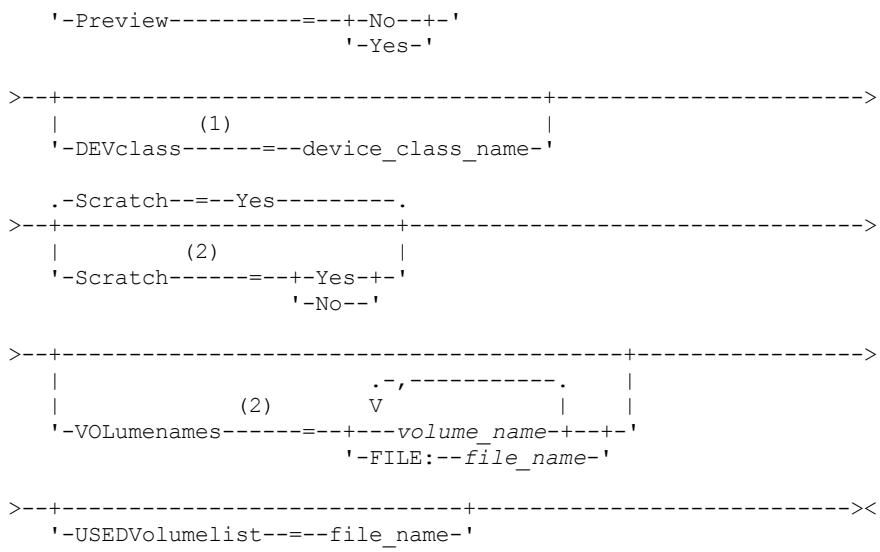
Use this command to export policy information from an IBM Spectrum Protect™ server to sequential media for later import to another server.

Privilege class

To issue this command, you must have system privilege.

Syntax





Notes:

1. If PREVIEW=NO, a device class must be specified.
2. If PREVIEW=NO and SCRATCH=NO, one or more volumes must be specified.

Parameters

domain_name
: Specifies the policy domains for which information is to be exported. This parameter is optional. The default is all policy domains. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

Preview
: Specifies whether to preview the results of the export operation, without exporting information. You can use this parameter to preview how many bytes of data are transferred so that you can determine how many volumes are required. This parameter supports the following values:

  No
  : Specifies that the policy information is to be exported. If you specify this value, you must also specify a device class.

  Yes
  : Specifies that the operation is previewed but not completed. Information is reported to the server console and the activity log. If you specify this value, you do not need to specify a device class.

  This parameter is optional. The default value is NO.

DEVclass
: Specifies the device class to which export data is to be written. This parameter is required if you specify PREVIEW=NO.

  You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the export runs, IBM Spectrum Protect cancels lower priority operations to make a drive available.

  Tip: You can export data to a storage pool on another server by specifying a device class whose device type is SERVER.

Scratch
: Specifies whether scratch volumes can be used. The default value is YES. You can specify one of the following values:

  Yes
  : Specifies that scratch volumes can be used for export. If you also specify a list of volumes, scratch volumes are used only if there is not enough space on the volumes specified.

  No
  : Specifies that scratch volumes cannot be used for export. To determine how many volumes you might need, you can run the command specifying PREVIEW=YES.

VOLumenames
: Specifies the volumes to be used to contain exported data. This parameter is optional, unless you specify SCRATCH=NO and PREVIEW=NO. If you do not specify a volume name, scratch volumes are used.

You can specify one of the following values:

volume_name
: Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

FILE:file_name
: Specifies the name of a file that contains a list of volumes. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when specifying volumes associated with the following device types:

For this device	Specify
Tape	1-6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: AIX Linux /imdata/mt1. Windows d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1-6 alphanumeric characters.
SERVER	1-250 alphanumeric characters.

USEDVolumelist
: Specifies the file where a list of volumes used in the export operation are stored. This parameter is optional.

This file can be used in the import operation. This file contains comment lines with the date and time the export was done, and the command issued to create the export.

Attention: If you specify an existing file, the file is overwritten.

Example: Export policy information to specific tape volumes

From the server, export policy information to tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class.

```
export policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Example: Export policy information to tape volumes listed in a file

From the server, export policy information to tape volumes that are listed in the following file:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

This file contains the following lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that these tape volumes be used by a device that is assigned to the MENU1 device class. Issue the following command:
AIX Linux

```
export policy devclass=menu1 volumenames=file:tapevol
```

Windows

```
export policy devclass=menu1 volumenames=file:tapevol.data
```

EXPORT POLICY (Export a policy directly to another server)

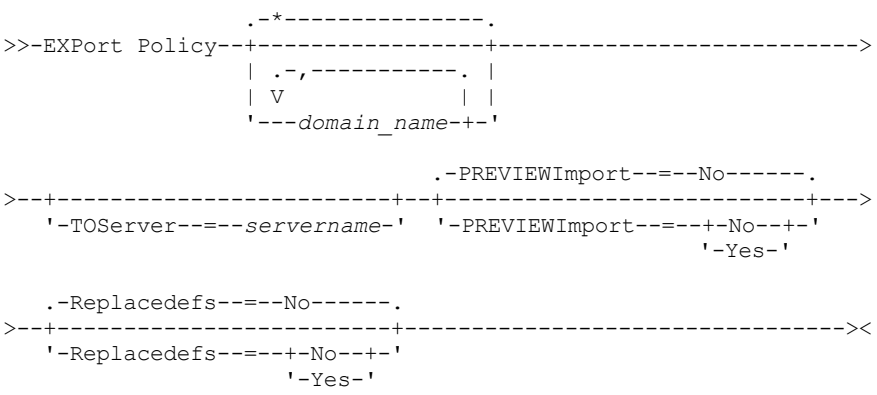
Use this command to export policy information directly to another server on the network. This results in an immediate import on the target server.

To monitor the progress of the import operation, you can issue a QUERY PROCESS command from the target server. See EXPORT ADMIN (Export administrator information) for a list of restrictions that apply to the export function.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

domain_name
: Specifies the policy domains for which information is to be exported. This parameter is optional. The default is all policy domains. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

TOServer
: Specifies the name of a server to which the export data is sent directly over the network for immediate import.
Important: The target server must be defined on the originating server with the DEFINE SERVER command. The administrator that issues the export command must be defined with the same administrator name and password and have system authority on the target server.

  When you specify TOSERVER, you cannot specify the DEVCLASS, VOLUMENAMES, and SCRATCH, USEDVOLUMELIST, and PREVIEW parameters.

PREVIEWImport
: Specifies whether to view how much data is transferred, without actually moving any data. This information can be used to determine how much storage pool space is required on the target server. The default is NO.
Valid values are:

  Yes
  : Specifies that you want to preview the results of the import operation on the target server, without importing the data. Information is reported to the server console and the activity log.

  No
  : Specifies that you want the data to be imported on the target server without previewing the results.

Replacedefs
: Specifies whether to replace definitions (not file data) on the server. The default is NO.

  Valid values are:

  Yes
  : Specifies that definitions are replaced on the server if definitions having the same name as those being imported exist on the target server.

  No
  : Specifies that imported definitions are skipped if their names conflict with definitions that are already defined on the target server.

Example: Export policy to another server

To export policy information directly to SERVERB, issue the following command:

```
export policy replacedefs=yes toserver=othersrv
```

EXPORT SERVER (Export server information)

Use this command to export all or part of the server control information and client file data (if specified) from the server to sequential media.

When you export server information to sequential media, you can later use the media to import the information to another server with a compatible device type.
Important: For commands that import administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect™ server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the IMPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

You also have the option of processing an export operation directly to another server on the network. This results in an immediate import process without the need for compatible sequential device types between the two servers.

You can export the following types of server information by issuing the EXPORT SERVER command:

- Policy domain definitions
- Policy set definitions
- Management class and copy group definitions
- Schedules defined for each policy domain
- Administrator definitions
- Client node definitions

You can optionally export the following types of data:

- File space definitions
- Access authorization information that pertains to the file spaces exported
- Backed-up, archived, and files that were migrated by an IBM Spectrum Protect for Space Management client

This command generates a background process that can be canceled by the CANCEL PROCESS command. If you export server information to sequential media, and the background process is canceled, the sequential media holding the exported data are incomplete and should not be used for importing data. If a server-to-server export background process is canceled, a partial import might result. Evaluate any imported data on the target server to determine whether you want to keep or delete the imported data. Review the import messages for details.

Issue the QUERY PROCESS command from the target server to monitor the progress of the import operation. Issue the QUERY EXPORT command to list all server-to-server export operations (that have a FILEDATA value other than NONE) that are running or suspended.

You can use the QUERY ACTLOG command to view the actual status information which indicates the size and the success or failure of the export operation.

The following restrictions apply to the export function:

- Export operations from a later version and release to an earlier version and release is not supported.
- Export operations between servers that are at the same version and release but with different fix packs might fail. For example, you cannot export from a V7.1.3 server to a V7.1.1 or earlier server.
- Exported data from a server with retention protection enabled is not protected by retention when it is imported to another server.
- Export processing excludes nodes of type network-attached storage (NAS).
- Exporting data to a Centera device class or importing data from a Centera device class is not supported. However, files that are stored in Centera storage pools can be exported and files that must be imported can be stored on a Centera storage device.

- The EXPORT NODE and EXPORT SERVER commands do not export data from a shred pool unless you explicitly allow it by setting the ALLOWSHREDDABLE parameter to the YES value. If this value is specified, and the exported data includes data from shred pools, that data cannot be shredded. A warning is not issued if the export operation includes data from shred pools.

- Incrementally exporting or importing the following types of client data to another IBM Spectrum Protect server is not supported:
  - VMware backups where full plus incremental backups need to be periodically, incrementally transferred to another server
  - Backups groups where full plus differential backups must be periodically, incrementally transferred to another server
  - Windows System State data that is periodically, incrementally transferred to another server

  Full export or import of this data to a new file system on the target is supported by exporting the entire file space that contains the data. The export must not use the FILEDATA=ALLACTIVE, FROMDATE, TODATE, or MERGEFILESPACES parameters.

  Using node replication to incrementally transfer this type of client data between two servers is optimal.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

The EXPORT SERVER command takes two forms: Export directly to another server on the network, or export to sequential media. The syntax and parameters for each form are defined separately.

Table 1. Commands related to EXPORT SERVER

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.
EXPORT ADMIN	Copies administrative information to external media or directly to another server.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT POLICY	Copies policy information to external media or directly to another server.
IMPORT SERVER	Restores all or part of the server from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
QUERY PROCESS	Displays information about background processes.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

- EXPORT SERVER (Export a server to sequential media)
  You can export all or part of the server control information and client file data from a server to sequential media so that this information can be imported to another server.
- EXPORT SERVER (Export server control information and client file data to another server)
  Use this command to export all or part of the server control information and client file data directly to another server on the network. This results in an immediate import on the target server.

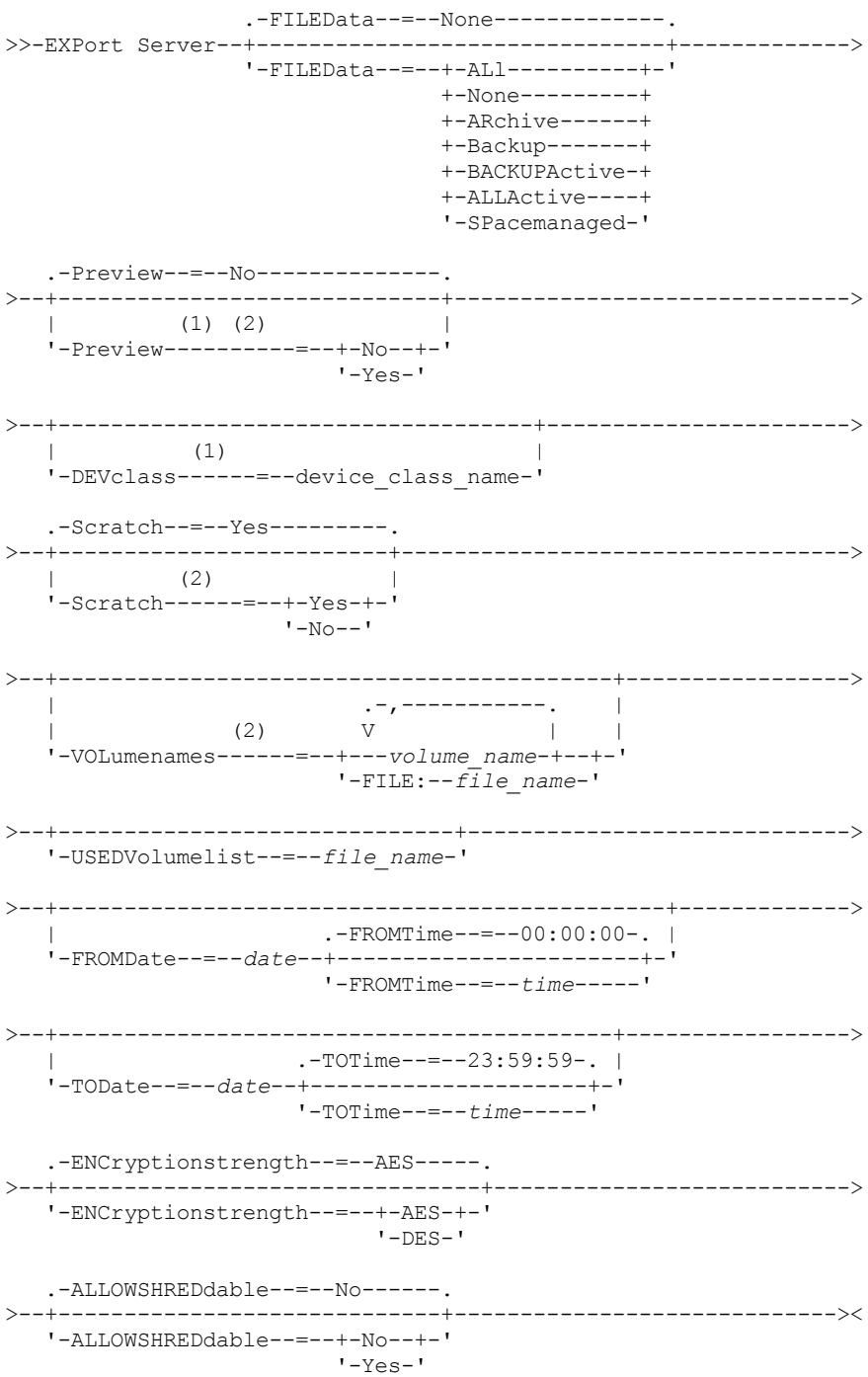
EXPORT SERVER (Export a server to sequential media)

You can export all or part of the server control information and client file data from a server to sequential media so that this information can be imported to another server.

Privilege class

To issue this command, you must have system privilege.

Syntax



Notes:

1. If PREVIEW=NO, a device class must be specified.
2. If PREVIEW=NO and SCRATCH=NO, one or more volumes must be specified.

Parameters

FILEData

Specifies the type of files that are exported for all nodes that are defined to the server. This parameter is optional. The default value is NONE.

If you are exporting to sequential media, the device class to access the file data is determined by the device class for the storage pool. If it is the same device class that is specified in this command, two drives are needed to export server information. The mount limit for the device class must be set to at least 2.

The following descriptions mention *active* and *inactive* backup file versions. An active backup file version is the most recent backup version for a file that still exists on the client workstation. All other backup file versions are called inactive copies. The following values are available:

ALl
: IBM Spectrum Protect™ exports all backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client.

None
: IBM Spectrum Protect does not export files, only definitions.

ARchive
: IBM Spectrum Protect exports only archived files.

Backup
: IBM Spectrum Protect exports only backup versions, whether the versions are active or inactive.

BACKUPActive
: IBM Spectrum Protect exports only active backup versions.

ALLActive
: IBM Spectrum Protect exports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client.

SPacemanaged
: IBM Spectrum Protect exports only files that were migrated by an IBM Spectrum Protect for Space Management client.

Preview
: Specifies whether you want to preview the results of the export operation, without exporting information. You can use this parameter to preview how many bytes of data are transferred so that you can determine how many volumes are required. This parameter supports the following values:

  No
  : Specifies that the server information is to be exported. If you specify this value, you must also specify a device class.

  Yes
  : Specifies that the operation is previewed but not completed. Information is reported to the server console and the activity log. If you specify this value, you do not need to specify a device class.

  This parameter is optional. The default value is NO.

DEVclass
: Specifies the device class to which export data is to be written. This parameter is required if you specify PREVIEW=NO.

  You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the export runs, IBM Spectrum Protect cancels lower priority operations to make a drive available.

  Tip: You can export data to a storage pool on another server by specifying a device class whose device type is SERVER.

Scratch
: Specifies whether scratch volumes can be used. The default value is YES. You can specify one of the following values:

  Yes
  : Specifies that scratch volumes can be used for export. If you also specify a list of volumes, scratch volumes are used only if there is not enough space on the volumes specified.

  No
  : Specifies that scratch volumes cannot be used for export. To determine how many volumes you might need, you can run the command specifying PREVIEW=YES.

VOLumenames
: Specifies the volumes to be used to contain exported data. This parameter is optional, unless you specify SCRATCH=NO and PREVIEW=NO. If you do not specify a volume name, scratch volumes are used.

  You can specify one of the following values:

volume_name
Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

FILE:file_name
Specifies the name of a file that contains a list of volumes. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when specifying volumes associated with the following device types:

For this device	Specify
Tape	1-6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: AIX Linux /imdata/mt1. Windows d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1-6 alphanumeric characters.
SERVER	1-250 alphanumeric characters.

USEDVolumelist
Specifies the file where a list of volumes used in the export operation are stored. This parameter is optional.

This file can be used in the import operation. This file contains comment lines with the date and time the export was done, and the command issued to create the export.

Attention: If you specify an existing file, the file is overwritten.

FROMDate
Specifies the earliest date for which files to be exported were stored on the server. Files that were stored on the server earlier than the specified date are not exported. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. IBM Spectrum Protect ignores the FROMDATE parameter when the FILEDATA parameter is set to NONE.
Directory processing: The FROMDATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.
Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. Group data on the node is, for example, virtual machine data or system state backup data. This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.
Use one of the following values to specify the date:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

If this parameter is not specified, IBM Spectrum Protect exports all objects stored before the TODATE parameter and as qualified by the FILEDATA parameter. If no TODATE parameter is specified, then all data as qualified by the FILEDATA parameter is exported.

When a server-to-server export operation uses a relative FROMDATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the FROMDATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

TODate

Specifies the latest date for files to be exported from the server. Files stored on the server on a date later than the TODATE value are not exported. TODATE only applies to client file data and does not affect other information that is being exported, such as policy.

- IBM Spectrum Protect ignores the TODATE parameter when the FILEDATA parameter is set to NONE.
- If a TODATE parameter is specified without a TOTIME parameter, the server exports all objects inserted on or before the day specified by the TODATE parameter.
- If you specified the FROMDATE parameter, the value of TODATE must be later than or equal to the FROMDATE value. If the TODATE and FROMDATE are equal, then the TOTIME parameter must be later that the FROMTIME parameter.
- The TODATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.

Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	10/15/2006
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

When a server-to-server export operation uses a relative TODATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the TODATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

FROMTime

Specifies the earliest time for which objects to be exported were stored on the server. When you specify FROMTIME, you must also use the FROMDATE parameter. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. Objects that were stored on the server before the specified time and date are not exported. IBM Spectrum Protect ignores the FROMTIME parameter when the FILEDATA parameter is set to NONE.

Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. An example of group data on the node is virtual machine data or system state backup data, This export is a result of incremental backup processing for the data. The incremental backup

processing can cause extra files that do not meet the filtering criteria to be exported so that there is a consistent image for the backup data.

The default value for this parameter when used with the FROMDATE parameter is midnight (00:00:00).

Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified. The FROMTIME+ can only be used with a FROMDATE before today.	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with FROMTIME=NOW+02:00 or FROMTIME=+02:00, the export operation only contains files that were put on the server after 7:00 on the FROMDATE that you specify.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW -02:00 **or** -02:00. If you issue this command at 5:00 with FROMTIME=NOW-02:00 or FROMTIME=-2:00, the export includes files that were put on the server after 3:00.

TOTime

Specifies the latest time that objects to be exported were stored on the server. You must specify the TODATE parameter in order to use the TOTIME parameter. TOTIME only applies to client file data and does not affect other information that is being exported, such as policy. IBM Spectrum Protect ignores the TOTIME parameter if the FILEDATA parameter is set to NONE.

The default value for this parameter, when used with the TODATE parameter, is midnight minus one second (23:59:59).

Important: The value of the TOTIME and TODATE parameters must be later than the FROMDATE and the FROMTIME value.
Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW+HH:MM **or**+HH:MM	The current time plus hours and minutes specified.	NOW+02:00 **or** +02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW+02:00, the export includes files that were stored from 01:00 until 07:00.
NOW-HH:MM **or**-HH:MM	The current time minus hours and minutes specified.	NOW-02:00 **or** -02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW-02:00, the export includes files that were stored from 01:00 until 03:00.

ENCryptionstrength

Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

AES
: Specifies the Advanced Encryption Standard.

DES
: Specifies the Data Encryption Standard.

ALLOWSHREDdable

Specifies whether data from a storage pool that enforces shredding is exported. This parameter is optional. The default value is NO. Possible values are:

No
: Specifies that data is not exported from a storage pool that enforces shredding.

Yes
: Specifies that data can be exported from a storage pool that enforces shredding. The data on the export media is not shredded.

Example: Export a server to specific tape volumes

From the server, export server information to tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class.

```
export server devclass=menu1
volumenames=tape01,tape02,tape03
```

Example: Export a server to tape volumes listed in a file

From the server, export server information to tape volumes that are listed in the following file:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

The file contains the following lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that the tape volumes be used by a device that is assigned to the MENU1 device class. Issue the following command:
AIX Linux

```
export server devclass=menu1 volumenames=file:tapevol
```

Windows

```
export server devclass=menu1 volumenames=file:tapevol.data
```

EXPORT SERVER (Export server control information and client file data to another server)

Use this command to export all or part of the server control information and client file data directly to another server on the network. This results in an immediate import on the target server.

Server-to-server export operations that have a FILEDATA value other than NONE can be restarted after the operation is suspended. The server saves the state and status of the export operation so that it may be restarted from the point at which the operation failed or was suspended. The export operation can be restarted at a later date by issuing the RESTART EXPORT command. These export operations can be manually suspended as well as restarted. Therefore, if an export fails, it is automatically suspended if it has completed the transmitting definitions phase.

An export operation is suspended when any of the following conditions is detected:

- A SUSPEND EXPORT command is issued for the running export operation
- Segment preemption - the file being read for export is deleted by some other process
- Communication errors on a server-to-server export
- No available mount points
- Necessary volumes are unavailable
- I/O errors encountered

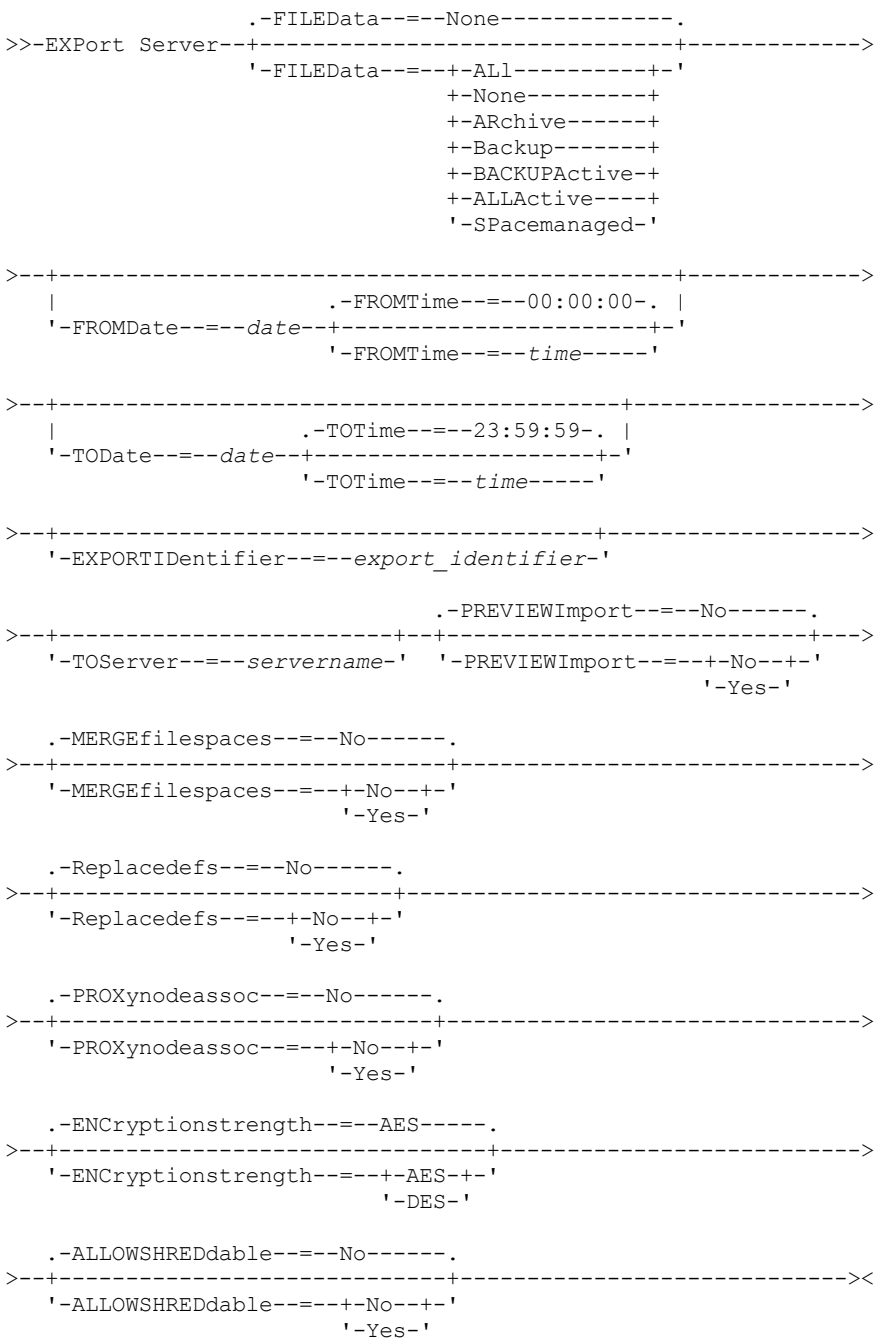
The export operation cannot be restarted if the export operation fails prior to transmitting the eligible node and filespace definitions to the target server. You must reenter the command to begin a new export operation.

Issue the QUERY PROCESS command from the target server to monitor the progress of the import operation. Issue the QUERY EXPORT command to list all server-to-server export operations (that have a FILEDATA value other than NONE) that are running or suspended. See EXPORT ADMIN (Export administrator information) for a list of restrictions that apply to the export function.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

FILEData

Specifies the type of files to export for all nodes defined to the server. This parameter is optional. The default value is NONE.

If you are exporting to sequential media: The device class to access the file data is determined by the device class for the storage pool. If it is the same device class specified in this command, IBM Spectrum Protect™ requires two drives to export server information. You must set the mount limit for the device class to at least 2.

The following descriptions mention active and inactive backup file versions. An active backup file version is the most recent backup version for a file that still exists on the client workstation. All other backup file versions are called inactive copies.

The values are:

ALl
: IBM Spectrum Protect exports all backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client.

None
: IBM Spectrum Protect does not export files, only definitions.

ARchive
: IBM Spectrum Protect exports only archived files.

Backup
: IBM Spectrum Protect exports only backup versions, whether they are active or inactive.

BACKUPActive
: IBM Spectrum Protect exports only active backup versions.

ALLActive
: IBM Spectrum Protect exports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client.

SPacemanaged
: IBM Spectrum Protect exports only files that were migrated by an IBM Spectrum Protect for Space Management client.

FROMDate
: Specifies the earliest date for which files to be exported were stored on the server. Files that were stored on the server earlier than the specified date are not exported. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. IBM Spectrum Protect ignores the FROMDATE parameter when the FILEDATA parameter is set to NONE.
Directory processing: The FROMDATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.
Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. Group data on the node is, for example, virtual machine data or system state backup data. This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported, so that there is a consistent image for the backup data.
Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

If this parameter is not specified, IBM Spectrum Protect exports all objects stored before the TODATE parameter and as qualified by the FILEDATA parameter. If no TODATE parameter is specified, then all data as qualified by the FILEDATA parameter is exported.

When a server-to-server export operation uses a relative FROMDATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the FROMDATE is specified as TODAY-1, the date that is used for

selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

TODate

Specifies the latest date for files to be exported from the server. Files stored on the server on a date later than the TODATE value are not exported. TODATE only applies to client file data and does not affect other information that is being exported, such as policy.

- IBM Spectrum Protect ignores the TODATE parameter when the FILEDATA parameter is set to NONE.
- If a TODATE parameter is specified without a TOTIME parameter, the server exports all objects inserted on or before the day specified by the TODATE parameter.
- If you specified the FROMDATE parameter, the value of TODATE must be later than or equal to the FROMDATE value. If the TODATE and FROMDATE are equal, then the TOTIME parameter must be later that the FROMTIME parameter.
- The TODATE parameter does not apply to directories. All directories in a file space are processed even if the directories were not backed up in the specified date range.

Use one of the following values to specify the date:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	10/15/2006
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY -3 **or** -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

When a server-to-server export operation uses a relative TODATE, for example, TODAY-1, and the operation is restarted at a later date, the restarted process still uses the date that was used during the original operation. For example, if a server-to-server export operation is started on 07/04/2009 and the TODATE is specified as TODAY-1, the date that is used for selecting files is 07/03/2009. If this same export operation is suspended and restarted ten days later (07/14/2009), the date that is used for selecting files is still 07/03/2009. This behavior ensures that the entire export operation uses the same cutoff date for selecting files to export.

FROMTime

Specifies the earliest time for which objects to be exported were stored on the server. When you specify FROMTIME, you must also use the FROMDATE parameter. This parameter only applies to client file data. This parameter does not affect other information that might be exported, for example, policy. Objects that were stored on the server before the specified time and date are not exported. IBM Spectrum Protect ignores the FROMTIME parameter when the FILEDATA parameter is set to NONE.
Important: If you have group data on the node that you are exporting, data that was backed up before the designated FROMDATE and FROMTIME can also be exported. An example of group data on the node is virtual machine data or system state backup data, This export is a result of incremental backup processing for the data. The incremental backup processing can cause extra files that do not meet the filtering criteria to be exported so that there is a consistent image for the backup data.

The default value for this parameter when used with the FROMDATE parameter is midnight (00:00:00).

Use one of the following values to specify the time:

Value	**Description**	**Example**

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified. The FROMTIME+ can only be used with a FROMDATE before today.	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with FROMTIME=NOW+02:00 or FROMTIME=+02:00, the export operation only contains files that were put on the server after 7:00 on the FROMDATE that you specify.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW -02:00 **or** -02:00. If you issue this command at 5:00 with FROMTIME=NOW-02:00 or FROMTIME=-2:00, the export includes files that were put on the server after 3:00.

TOTime

Specifies the latest time that objects to be exported were stored on the server. You must specify the TODATE parameter in order to use the TOTIME parameter. TOTIME only applies to client file data and does not affect other information that is being exported, such as policy. IBM Spectrum Protect ignores the TOTIME parameter if the FILEDATA parameter is set to NONE.

The default value for this parameter, when used with the TODATE parameter, is midnight minus one second (23:59:59).

Important: The value of the TOTIME and TODATE parameters must be later than the FROMDATE and the FROMTIME value. Use one of the following values to specify the time:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW+HH:MM **or**+HH:MM	The current time plus hours and minutes specified.	NOW+02:00 **or** +02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW+02:00, the export includes files that were stored from 01:00 until 07:00.
NOW-HH:MM **or**-HH:MM	The current time minus hours and minutes specified.	NOW-02:00 **or** -02:00. If you issue this command at 05:00 with FROMTIME=01:00 and TOTIME=NOW-02:00, the export includes files that were stored from 01:00 until 03:00.

TOServer

Specifies the name of a server to which the export data is sent directly over the network for immediate import.
Important: The target server must be defined on the originating server with the DEFINE SERVER command. The administrator that issues the export command must be defined with the same administrator name and password and have system authority on the target server.

When you specify TOSERVER, you cannot specify the DEVCLASS, VOLUMENAMES, and SCRATCH, USEDVOLUMELIST, and PREVIEW parameters.

PREVIEWImport

Specifies whether to view how much data is transferred, without actually moving any data. This information can be used to determine how much storage pool space is required on the target server. The default is NO.
Valid values are:

Yes

Specifies that you want to preview the results of the import operation on the target server, without importing the data. Information is reported to the server console and the activity log.

No

Specifies that you want the data to be imported on the target server without previewing the results.

MERGEfilespaces
Specifies whether IBM Spectrum Protect merges client files into existing file spaces on the target server (if they exist), or if IBM Spectrum Protect generates new file space names. The default is NO.

Valid values are:

Yes
Specifies that imported data on the target server is merged with the existing file space, if a file space with the same name exists on the target server.
No
Specifies that IBM Spectrum Protect generates a new file space name for imported data on the target server if file spaces with the same name exists.

Replacedefs
Specifies whether to replace definitions (not file data) on the server. The default is NO.

Valid values are:

Yes
Specifies that definitions are replaced on the server if definitions having the same name as those being imported exist on the target server.
No
Specifies that imported definitions are skipped if their names conflict with definitions that are already defined on the target server.

PROXynodeassoc
Specifies if proxy node associations are exported. This parameter is optional. The default value is NO.

ENCryptionstrength
Indicates which algorithm to use to encrypt passwords when exporting administrative and node records. This parameter is optional. The default value is AES. If you are exporting to a server that does not support AES, specify DES. You can specify one of the following values:

AES
Specifies the Advanced Encryption Standard.
DES
Specifies the Data Encryption Standard.

ALLOWSHREDdable
Specifies whether data from a storage pool that enforces shredding is exported. This parameter is optional. The default value is NO. Possible values are:

No
Specifies that the server does not allow data to be exported from a storage pool that enforces shredding.
Yes
Specifies that the server allows data to be exported from a storage pool that enforces shredding. The data on the export media will not be shredded.

Important: After an export operation finishes identifying files for export, any changes to the storage pool ALLOWSHREDABLE value is ignored. An export operation that is suspended retains the original ALLOWSHREDABLE value throughout the operation. You might want to consider canceling your export operation if changes to the storage pool ALLOWSHREDABLE value jeopardize the operation. You can reissue the export command after any needed cleanup.

EXPORTIDentifier
This optional parameter specifies the name that you selected to identify this export operation. If you do not specify a command name, the server generates one for you. The export identifier name cannot be more than 64 characters, cannot contain wildcard characters, and is not case sensitive. You can use the identifier name to reference export operations in the QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT, or CANCEL EXPORT commands. EXPORTIDENTIFIER is ignored if FILEDATA=NONE or if PREVIEWIMPORT=YES.

If you are specifying the EXPORTIDENTIFIER parameter, you must specify the TOSERVER parameter.

Example: Export server information directly to another server

To export server information directly to SERVERB, issue the following command.

```
export server filedata=all toserver=serverb
```

Example: Export server information directly to another server using a date range

To export directly to SERVERB between February 1, 2009 and today, issue the following command.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

Example: Export server information and client file data directly to another server using a date and time range

To export directly to SERVERB from 8:00 a.m. on February 1, 2009 until today at 8:00 a.m., issue the following command.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

EXTEND DBSPACE (Increase space for the database)

Use this command to increase space for the database by adding directories for the database to use.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

When you issue the EXTEND DBSPACE command, directories are added to the database. With the default parameter settings, data is redistributed across all database directories, and storage space is reclaimed. This action improves parallel I/O performance and makes the new directory space available for immediate use.

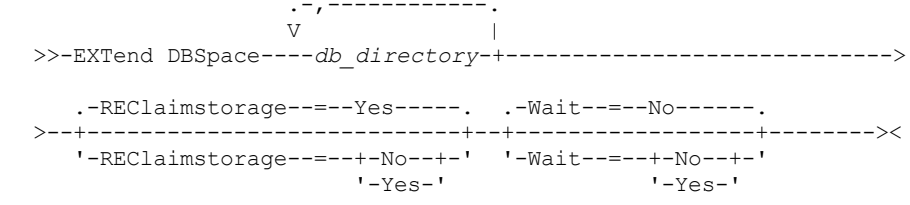
If you do not want to redistribute data when you add new directories, you can specify `RECLAIMSTORAGE=NO`. If you specify `No` for this parameter, all space in existing directories is filled before new directories are used. You can redistribute data and reclaim space later, but you must complete the manual procedure for this task by using DB2 commands.

Restriction: Redistribution of data and reclaiming of space as part of an operation to extend database space works only with DB2 Version 9.7 or later table spaces. The table spaces are created when you format a new IBM Spectrum Protect™ Version 6.2 or later server. If you upgraded or restored your IBM Spectrum Protect server from V6.1, you cannot redistribute data or reclaim space. You must issue the EXTEND DBSPACE command with `RECLAIMSTORAGE=NO`.
Important: The redistribution process uses considerable system resources, so ensure that you plan ahead when you want to add space to the database. Review the following guidelines:

- Complete the process when the server is not handling a heavy workload.
- The time that is required to redistribute data and reclaim space might vary. It is affected by factors such as the file system layout, the ratio of new paths to existing storage paths, server hardware, and concurrent operations. To get a rough estimate, you can try the operation with a small IBM Spectrum Protect database on a lab system. Use your results as a reference to estimate the time that is required for the procedure.
- Do not interrupt the redistribution process. If you try to stop it, for example, by halting the process that is completing the work, you must stop and restart the DB2® server. When the server is restarted, it will go into crash recovery mode, which takes several minutes, after which the redistribution process resumes.

After an operation to extend the database space is complete, halt and restart the server to fully use the new directories. If the existing database directories are nearly full when a new directory is added, the server might encounter an out of space condition (reported in the db2diag.log). You can fix the out of space condition by halting and restarting the server.

Syntax



Parameters

db_directory (Required)

Specifies the directories for database storage. The directories must be empty and accessible by the user ID of the database manager. A directory name must be a fully qualified name and cannot exceed 175 characters in length. Enclose the name in quotation marks if it contains embedded blanks, an equal sign, or other special characters. If you are specifying a list of directories for database storage, the maximum length of the list can be 1400 characters.

Windows Restriction: You cannot specify Universal Naming Convention (UNC) paths.

Tip: Specify directories that are the same size as existing directories to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

RECLaimstorage

Specifies whether data is redistributed across newly created database directories and space is reclaimed from the old storage paths. This parameter is optional. The default value is Yes.

Unless you specify `WAIT=YES`, the operation is completed as a background process.

Yes

Specifies that data is redistributed so that new directories are available for immediate use.
Important: The redistribution process uses considerable system resources so ensure that you plan ahead.

After the process starts, messages are issued to inform you about the progress. You can use the QUERY PROCESS command to monitor the operation. To cancel the process, you can use the CANCEL PROCESS command, but if a data redistribution operation is in progress, it completes before the process is stopped.

No

Specifies that data is not redistributed across database directories and storage space is not reclaimed when space is added for the database.

Wait

Specifies whether this command is processed in the background or foreground.

No

Specifies background processing. The default is NO.

Yes

Specifies foreground processing.

AIX Linux You cannot specify YES from the server console.

AIX Linux

Example: Add directories to the storage space for the database, redistribute data, and reclaim storage

Add two directories (/tsm_db/stg1 and tsm_db/stg2) under the /tsm_db directory to the storage space for the database. Issue the command:

```
extend dbspace /tsm_db/stg1,/tsm_db/stg2
```

Windows

Example: Add drives to the storage space for the database, redistribute data, and reclaim storage

Add drives D and E to the storage space for the database. Issue the command:

```
extend dbspace D:,E:
```

Related commands

Table 1. Commands related to EXTEND DBSPACE

Command	Description
DSMSERV EXTEND DBSPACE	Adds directories to increase space for use by the database.

Command	Description
QUERY DB	Displays allocation information about the database.
QUERY DBSPACE	Displays information about the storage space defined for the database.

Related tasks:
Managing inventory capacity

GENERATE commands

Use the GENERATE commands for backup sets for a selected filespace or client node.

- GENERATE BACKUPSET (Generate a backup set of Backup-Archive Client data)
- GENERATE BACKUPSETTOC (Generate a table of contents for a backup set)
- AIX Linux Windows GENERATE DEDUPSTATS (Generate data deduplication statistics)

GENERATE BACKUPSET (Generate a backup set of Backup-Archive Client data)

Use this command to generate a backup set for a Backup-Archive Client node. A *backup set* is a collection of a Backup-Archive Client's active backed up data, which is stored and managed as a single object, on specific media, in server storage. Although you can create a backup set for any client node, a backup set can be used only by a Backup-Archive Client.

Restriction: A backup set in "deduplication format" has that designation as a result of a GENERATE BACKUPSET command with at least one of the following specifications:

- Includes a node at Backup-Archive Client Version 6.1.x (at least V6.1.0 but less than V6.2.0).
- Includes a node that has one or mode nodes that are authorized to act as a proxy. At least one of those proxy nodes is at Backup-Archive Client V6.1.x.

Backup sets in the deduplication format can be restored only by the V6.1.2 or later Backup-Archive Client. Backup-Archive Clients before V6.1.2 cannot restore from a backup set that is in the deduplication format.
A backup set in the "distributed deduplication format" has that designation as a result of a GENERATE BACKUPSET command with at least one of the following specifications:

- Includes a node at Backup-Archive Client level V6.2.0 or later.
- Includes a node that has one or mode nodes that are authorized to act as a proxy. At least one of those proxy nodes is at Backup-Archive Client V6.2.0.

Backup sets in the distributed deduplication format can be restored only by the V6.2.0 or later Backup-Archive Client.
Restriction: You cannot generate a backup set with files that were backed up to IBM Spectrum Protect™ using NDMP. However, you can create a backup set with files that were backed up using NetApp SnapShot Difference.

The server creates copies of active versions of a client's backed up objects that are within the one-or-more file spaces specified with this command. The server then consolidates them onto sequential media. Currently, the backup object types that are supported for backup sets include directories and files only.

The backup-archive client node can restore its backup set from the server and from the media to which the backup set was written.

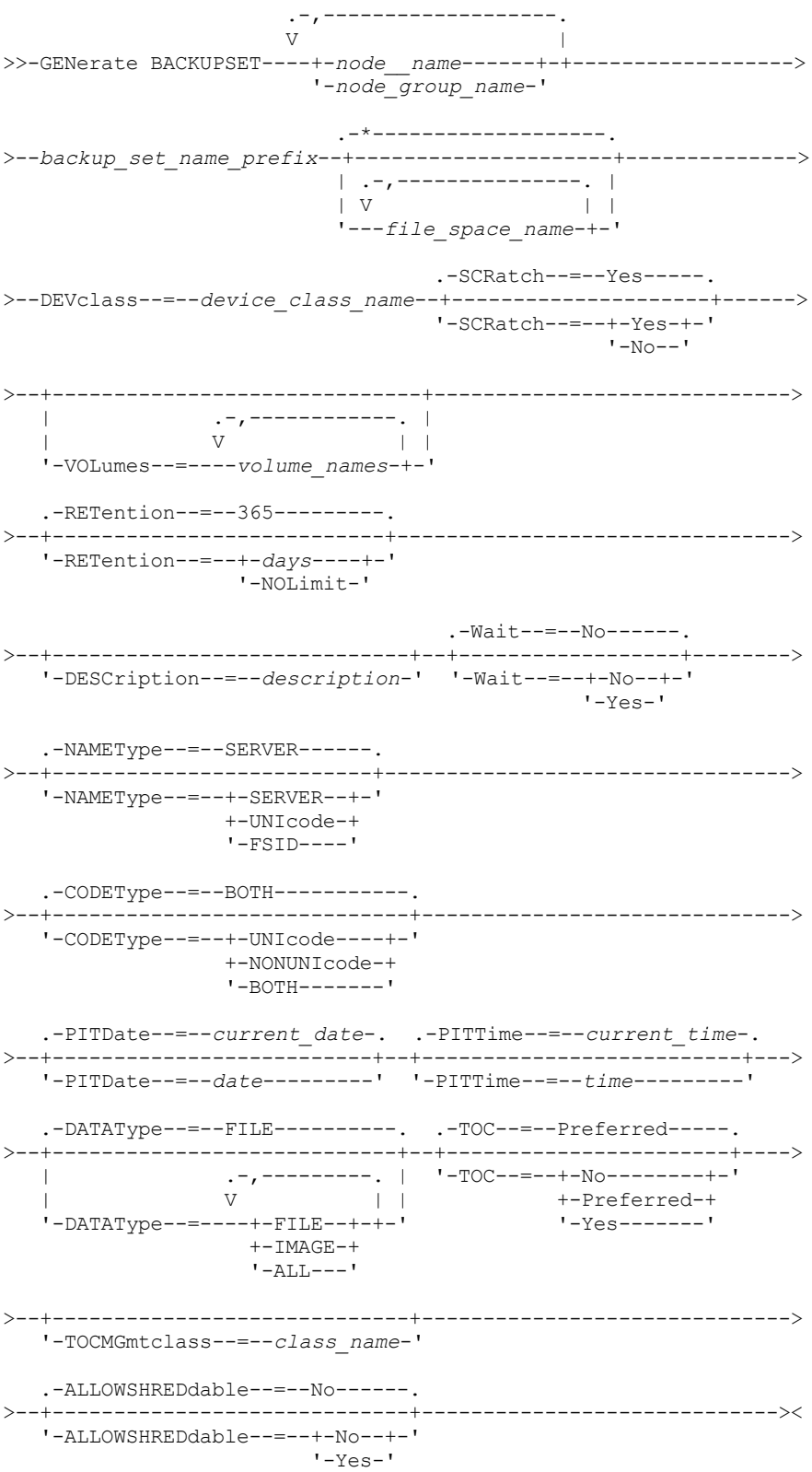
This command generates a background process that can be canceled with the CANCEL PROCESS command. If the background process created by this command is canceled, the media might not contain a complete backup set. You can use the QUERY PROCESS command to show information about the background process that is created by this command.

Tip: When IBM Spectrum Protect generates a backup set, you can improve performance if the primary storage pools containing the client data are collocated. If a primary storage pool is collocated, client node data is likely to be on fewer tape volumes than it would be if the storage pool were not collocated. With collocation, less time is spent searching database entries, and fewer mount operations are required.

Privilege class

To issue this command, you must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax



Parameters

node_name or node_group_name (Required)

Specifies the name of the client node and node groups whose data is contained in the backup set. To specify multiple node names and node group names, separate the names with commas and no intervening spaces. You can use wildcard characters with node names but not with node group names. When multiple node names are specified, the server generates a backup set for each node and places all of the backup sets together on a single set of output volumes.

backup_set_name_prefix (Required)
Specifies the name of the backup set for the client node. The maximum length of the name is 30 characters.

When you select a name, IBM Spectrum Protect adds a suffix to construct your backup set name. For example, if you name your backup set *mybackupset*, IBM Spectrum Protect adds a unique number such as 3099 to the name. The backup set name is then identified to IBM Spectrum Protect as *mybackupset.3099*. To later show information about this backup set, you can include a wildcard with the name, such as *mybackupset.** or specify the fully qualified name, such as *mybackupset.3099*.

When multiple node names or node group names are specified, the server generates a backup set for each node or node group and places all the backup sets on a single set of output volumes. Each backup set is given the same fully qualified name consisting of the *backup_set_name_prefix* and a suffix determined by the server.

file_space_name
Specifies the names of one or more file spaces that contain the data to be included in the backup set. This parameter is optional. The file space name that you specify can contain wildcard characters. You can specify more than one file space by separating the names with commas and no intervening spaces. If you do not specify a file space, data from all the client nodes backed-up and active file spaces is included in the backup set.

For a server that has clients with support for Unicode-enabled file spaces, you can enter either a file space name or a file space ID (FSID). If you enter a file space name, you might need to have the server convert the file space name that you enter. For example, you might need to have the server convert the name that you enter from the server's code page to Unicode. See the NAMETYPE parameter for details. If you do not specify a file space name, or specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

DEVclass (Required)
Specifies the name of the device class for the volumes to which the backup set is written. The maximum length of the name is 30 characters.
Restriction: You cannot specify a device class with a device type of NAS or CENTERA.

SCRatch
Specifies whether to use scratch volumes for the backup set. If you include a list of volumes using the VOLUMES parameter, the server uses scratch volumes only if the data cannot be contained in the volumes you specify. The default is SCRATCH=YES. The values are:

YES
Specifies to use scratch volumes for the backup set.

NO
Specifies not to use scratch volumes for the backup set.

VOLumes
Specifies the names of one or more volumes that will contain the backup set. This parameter is optional. You can specify more than one volume by separating each volume with a comma, with no intervening spaces.

If you do not specify this parameter, scratch volumes are used for the backup set.

RETention
Specifies the number of days to retain the backup set on the server. You can specify an integer from 0 to 30000. The default is 365 days. The values are:

days
Specifies the number of days to retain the backup set on the server.

NOLimit
Specifies that the backup set should be retained on the server indefinitely.

If you specify NOLIMIT, the server retains the volumes containing the backup set forever, unless a user or administrator deletes the volumes from server storage.

DESCription
Specifies the description to associate with the backup set. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. The values are:

Yes

Specifies the command processes in the foreground. Messages that are created are not displayed until the command completes processing. You cannot specify WAIT=YES from the server console.

No

Specifies that the command processes in the background. Use the QUERY PROCESS command to monitor the background processing of this command.

NAMEType

Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for Unicode-enabled file spaces. You can use this parameter for IBM Spectrum Protect clients using Windows, NetWare, or Macintosh OS X operating systems.

Use this parameter only when you enter a partly or fully qualified file space name. The default value is SERVER. Possible values are:

SERVER

The server uses the server's code page to interpret the file space names.

UNIcode

The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has a problem accessing system conversion routines.

FSID

The server interprets the file space names as their file space IDs (FSIDs).
Important: Use care when specifying this parameter if multiple node names are also specified. Different nodes might use the same file space ID for different file spaces, or different file space IDs for the same file space name. Therefore, specifying a file space ID as the file space names can result in the wrong data being written to the backup set for some nodes.

CODEType

Specify what type of file spaces are to be included in the operation. The default is BOTH, meaning that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name or when you do not specify any file space names. Possible values are:

UNIcode

Include only file spaces that are in Unicode.

NONUNIcode

Include only file spaces that are not in Unicode.

BOTH

Include file spaces regardless of code page type.

PITDate

Specifies that files that were active on the specified date and that are still stored on the IBM Spectrum Protect server are to be included in the backup set, even if they are inactive at the time you issue the command. This parameter is optional. The default is the date on which the GENERATE BACKUPSET command is run. You can specify the date using one of the following values:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days**or**-days	The current date minus days specified	TODAY-7 or -7. To include files that were active a week ago, specify PITDATE=TODAY-7 or PITDATE=-7
EOLM (End Of Last Month)	The last day of the previous month.	EOLM

Value	Description	Example
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

PITTime

Specifies that files that were active on the specified time and that are still stored on the IBM Spectrum Protect server are to be included in the backup set, even if they are inactive at the time you issue the command. This parameter is optional. IF a PITDate was specified, the default is midnight (00:00:00); otherwise the default is the time at which the GENERATE BACKUPSET command is started. You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified PIT date	12:33:28
NOW	The current date on the specified PIT date	NOW
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified PIT date	NOW+03:00 or +03:00 If you issue this command at 9:00 with PITTIME=NOW+03:00 or PITTIME=+03:00. IBM Spectrum Protect includes files that were active at 12:00 on the PIT date.

DATAType

Specifies that backup sets containing the specified types of data that are to be generated. This parameter is optional. The default is that file level backup sets are to be generated. To specify multiple data types, separate data types with commas and no intervening spaces.

The server generates a backup set for each data type and places all the backup sets on a single set of output volumes. Each backup set is given the same fully qualified name consisting of the *backup_set_name_prefix* and a suffix determined by the server. However, each backup set has a different data type, as shown by the QUERY BACKUPSET command. Possible values are:

ALL
: Specifies that backup sets for all types of data (file level, image, and application) that have been backed up on the server are to be generated.

FILE
: Specifies that a file level backup set is to be generated. File level backup sets contain files and directories that are backed up by the backup client. If no files or directories have been backed up by the backup client, a file level backup set is not generated. This is the default.

IMAGE
: Specifies that an image backup set is to be generated. Image backup sets contain images that are created by the backup client BACKUP IMAGE command. Image backup sets are generated only if an image has been backed up by the backup client.

TOC

Specifies whether a table of contents (TOC) is saved for each file level backup set. Tables of contents are always saved for backup sets containing image or application data. The TOC parameter is ignored when generating image and application backup sets. A table of contents will always be generated for image and application backup sets.
Consider the following in determining whether you want to save a table of contents:

- If a table of contents is saved for a backup set, you can use the IBM Spectrum Protect web backup-archive client to examine the entire file system tree and choose files and directories to restore. To create a table of contents, you must define the TOCDESTINATION attribute in the backup copy group for the management class that is specified by

the TOCMGMTCLASS parameter. Creating a table of contents requires additional processing, storage pool space, and possibly a mount point during the backup set operation.

- If a table of contents is not saved for a backup set, you can still restore individual files or directory trees using the backup-archive client RESTORE BACKUPSET command, if you know the fully qualified name of each file or directory to be restored.

To display the contents of backup sets, you can also use the QUERY BACKUPSETCONTENTS command.

This parameter is optional. Possible values are:

No
: Specifies that table of contents information is not saved for file level backup sets.

Preferred
: Specifies that table of contents information should be saved for file level backup sets. This is the default. However, a backup set does not fail just because an error occurs during creation of the table of contents.

Yes
: Specifies that table of contents information must be saved for each file level backup set. A backup set fails if an error occurs during creation of the table of contents.

TOCMGmtclass
: Specifies the name of the management class to which the table of contents should be bound. If you do not specify a management class, the table of contents is bound to the default management class for the policy domain to which the node is assigned. In this case, creation of a table of contents requires that you define the TOCDESTINATION attribute in the backup copy group for the specified management class.

ALLOWSHREDdable
: Specifies whether data from a storage pool that enforces shredding is included in the backup set. This parameter is optional. Possible values are:

No
: Specifies that data from a storage pool that enforces shredding is not included in the backup set. This is the default.

Yes
: Specifies that data from a storage pool that enforces shredding can be included in the backup set. The data on the backup set media will not be shredded.

Example: Generate a backup set for a file space

Generate a backup set of a file space that is called /srvr that belongs to client node JANE. Name the backup set PERS_DATA and retain it for 75 days. Specify that volumes VOL1 and VOL2 contain the data for the backup set. The volumes are to be read by a device that is assigned to the AGADM device class. Include a description.

```
generate backupset jane pers_data /srvr devclass=agadm
retention=75 volumes=vol1,vol2
description="area 51 base image"
```

Example: Generate a backup set of a Unicode-enabled file space

Generate a backup set of the Unicode-enabled file space, \\joe\c$, that belongs to client node JOE. Name the backup set JOES_DATA. Specify that volume VOL1 contain the data for the backup set. The volume is to be read by a device that is assigned to the AGADM device class. Have the server convert the \\joe\c$ file space name from the server code page to the UTF-8 code page.

```
generate backupset joe joes_data \\joe\c$ devclass=agadm
volumes=vol1 nametype=unicode
```

Related commands

Table 1. Commands related to GENERATE BACKUPSET

Command	Description
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.

Command	Description
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
QUERY BACKUPSET	Displays backup sets.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
QUERY NODEGROUP	Displays information about node groups.
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE NODEGROUP	Updates the description of a node group.

GENERATE BACKUPSETTOC (Generate a table of contents for a backup set)

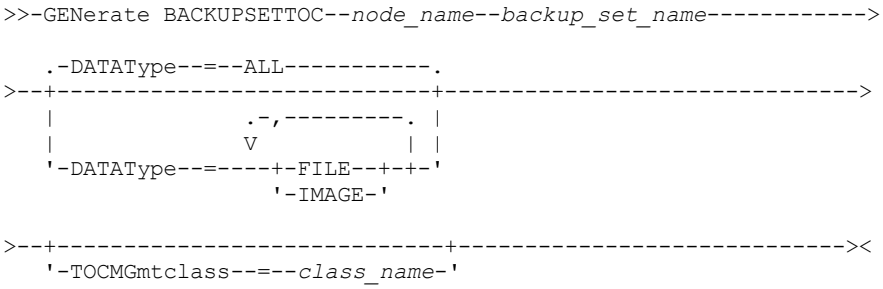
Use this command to generate a table of contents for a backup set that does not already have one. The backup-archive client uses the table of contents to display the backup set, which allows users to select individual files to be restored from the backup set.

Creating a table of contents for a backup set requires storage pool space and possibly one or more mount points during the creation operation.

Privilege class

To issue this command, you must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax



Parameters

node_name (Required)
: Specifies the name of the client node whose data is contained in the backup set. You cannot use wildcard characters to specify a name, nor can you specify a list of client node names.

backup_set_name (Required)
: Specifies the name of the backup set for the client node. You cannot use wildcard characters to specify a name, nor can you specify a list of backup set names.

DATAType
: Specifies the type of data to be included in the table of contents. This parameter is optional. By default, all data is included. To specify multiple data types, separate the data types with commas and no intervening spaces. Possible values are:

ALL
: Specifies that the table of contents includes all types of data (file-level, image, and application) stored in the backup set. This is the default.

FILE
: Specifies that the table of contents includes only file-level data. File-level data consists of files and directories backed up by the backup-archive client. If the backup set contains no files or directories, the table of contents is not generated.

IMAGE
: Specifies that the table of contents will include only image backups. Image backups consist of file system images created by the backup client BACKUP IMAGE command. If the backup set contains no image backups, the table of contents will not be generated.

TOCMGmtclass
: Specifies the name of the management class to which the table of contents should be bound. If you do not specify a management class, the table of contents is bound to the default management class for the policy domain to which the node is assigned. If you create a table of contents you must define the TOCDESTINATION attribute in the backup copy group for the specified management class.

Example: Generate a table of contents

Generate a table of contents for a backup set named PROJX_DATA that contains the data for client node GARY. The table of contents is to be bound to the default management class.

```
generate backupsettoc gary projx_data
```

Related commands

Table 1. Commands related to GENERATE BACKUPSETTOC

Command	Description
COPY ACTIVEDATA	Copies active backup data.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE NODEGROUP	Updates the description of a node group.

AIX | Linux | Windows

GENERATE DEDUPSTATS (Generate data deduplication statistics)

Use this command to generate data deduplication statistics for a directory-container storage pool or a cloud-container storage pool to determine data deduplication performance.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool.

Syntax

Parameters

pool_name (Required)
: Specifies the name of the storage pool that is reported in the data deduplication statistics. You can specify up to 30 characters for the storage pool name. If you specify more than 30 characters, the command fails.
Restriction: You can specify only directory-container storage pools or cloud storage pools.

node_name or node_group_name (Required)
: Specifies the name of the client node or defined group of client nodes that is reported in the data deduplication statistics. You can also specify a combination of client node names and client-node group names. To specify multiple client node names or client-node group names, separate the names with commas with no intervening spaces. You can use wildcard characters with client node names but not with client-node group names. The specified value can have a maximum of 1024 characters.

filespace_name or FSID
: Specifies the names of one or more file spaces for which data deduplication statistics are collected. This parameter is optional. You can use wildcard characters to specify this name. The specified value can have a maximum of 1024 characters. An asterisk is the default. You can specify one of the following values:

  *
  : Specify an asterisk (*) to show information for all file spaces or IDs.

  filespace_name
  : Specifies the name of the file space. You can specify more than one file space by separating the names with commas and no intervening spaces.

  FSID
  : Specifies the name of a file space identifier. This parameter is valid for clients with file spaces that are in Unicode format. Specify more than one file space by separating the names with commas and no intervening spaces.

  For clients with file spaces that are in Unicode format, you can enter either a file space name or an FSID. If you enter a file space name, the server might have to convert the file space name that you enter. For example, the server might have to convert the name that you enter from the server's code page to Unicode.
  Restrictions: The following restrictions apply to file space names and FSIDs:

  - You must specify a node name if you specify a file space name.
  - Do not specify both file space names and FSIDs on the same command.

CODEType
Specifies what type of file spaces to include in the record. The default value is BOTH, which specifies that file spaces are included regardless of code page type. Use this parameter only when you enter an asterisk to display information about all file spaces. This parameter is optional. Specify one of the following values:

UNIcode
Include file spaces that are in Unicode format.
NONUNIcode
Include file spaces that are not in Unicode format.
BOTH
Include file spaces regardless of code page type. This is the default.

MAXPRocess
Specifies the maximum number of parallel processes to generate statistics for a container in a directory-container or cloud-container storage pool. This parameter is optional. Enter a value in the range 1 - 99. The default value is 4.
NAMEType
Specifies how you want the server to interpret the file space names that you enter. Use this parameter when IBM Spectrum Protect™ clients have file spaces that are in Unicode format, and are on Windows, NetWare, or Macintosh OS X operating systems. This parameter is optional.
This parameter is required if you specify a node name and a file space name or FSID.
Restriction: When you specify this parameter, the file space name cannot contain an asterisk.

Specify one of the following values:

SERVER
The server uses the server's code page to interpret the file space names. This is the default.
UNIcode
The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the characters in the name and the server's code page.
Tip: Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.
FSID
The server interprets the file space names as their FSIDs.

Wait
Specifies whether the data deduplication statistics are generated in the foreground or background. This parameter is optional. You can specify one of the following values:

No
Specifies that the operation is completed in the background. You can continue with other tasks while the command is processing. Messages that are related to the background process are displayed in the activity log file or the server console, depending on where the messages are logged. This is the default value.
Yes
Specifies that the operation is completed in the foreground. It might take a long time to complete the operation. The operation must end before you can continue with other tasks. Messages are displayed in the activity log file or the server console, or both, depending on where the messages are logged.
Restriction: You cannot specify the WAIT=YES parameter from the server console.

DESCription
Specifies a description of the generated statistics. This parameter is optional.

Example: Generate data deduplication statistics for a file space

Generate data deduplication statistics for a file space that is called /srvr that belongs to a directory-container storage pool, POOL1, that is stored on client node NODE1.

```
generate dedupstats pool1 node1 /srvr
```

Example: Generate data deduplication statistics for a Unicode-enabled file space

Generate data deduplication statistics for a Unicode-enabled file space that is called \\abc\c$ that belongs to client node NODE2. Convert the \\abc\c$ file space name from the server code page to the UTF-8 code page.

```
generate dedupstats node2 \\abc\c$ nametype=unicode
```

Related commands

Table 1. Commands related to GENERATE DEDUPSTATS

Command	Description
AIX Linux Windows DELETE DEDUPSTATS	Deletes data deduplication statistics.
AIX Linux Windows QUERY DEDUPSTATS	Displays data deduplication statistics.

GRANT commands

Use the GRANT command to grant appropriate privileges or access.

- GRANT AUTHORITY (Add administrator authority)
- GRANT PROXYNODE (Grant proxy authority to a client node)

GRANT AUTHORITY (Add administrator authority)

Use this command to grant an administrator one or more administrative privilege classes, and authority to access client nodes.

You cannot grant restricted privilege to an unrestricted policy or unrestricted storage administrator. You must use the REVOKE AUTHORITY command to remove the administrator's unrestricted privilege, then use this command to grant restricted privilege to the administrator.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-GRant AUTHority--admin_name---------------------------------->

                   .-,---------------.
           (1)     V                 |
>--CLasses------=----+-SYstem------+-+-------------------------->
                     +-Policy------+
                     +-STorage-----+
                     +-Operator----+
                     '-Node--| A |-'

>--+-----------------------------+------------------------------>
   |             .-,-----------. |
   |             V             | |
   '-DOmains--=----domain_name-+-'

>--+-------------------------------+-------------------------><
   |                   .-,---------. |
   |          (1)      V           | |
   '-STGpools------=----pool_name-+-'

A

   .-AUTHority--=--Access-----.
|--+-------------------------+--+-DOmains--=--domain_name-+----|
   '-AUTHority--=--+-Access-+-'  '-NOde--=--node_name------'
                   '-Owner--'
```

Notes:

1. You must specify one or more of these parameters.

Parameters

admin_name (Required)

Specifies the name of the administrator being granted an administrative privilege class.

CLasses

Specifies one or more privilege classes to grant to an administrator. This parameter is required, except when you specify the STGPOOLS parameter. You can specify more than one privilege class by separating each with a comma. Possible classes are:

SYstem

Specifies that you want to grant system privilege to an administrator. A system administrator has the highest level of authority in IBM Spectrum Protect™. A system administrator can issue any administrative command and has authority to manage all policy domains and all storage pools. Do not specify additional privilege classes or the DOMAINS or STGPOOLS parameters when granting system privilege to an administrator. Only a system administrator can grant authority to other administrators.

Policy

Specifies that you want to grant policy privilege to an administrator. If you do not specify the DOMAINS parameter, unrestricted policy privilege is granted. An unrestricted policy administrator can issue commands that affect all existing policy domains as well as any policy domains that are defined in the future. An unrestricted policy administrator cannot define, delete, or copy policy domains. Use the GRANT AUTHORITY command with CLASSES=POLICY and no DOMAINS parameter to upgrade a restricted policy administrator to an unrestricted policy administrator.

STorage

Specifies that you want to grant storage privilege to an administrator. If the STGPOOLS parameter is not specified, unrestricted storage privilege is granted. An unrestricted storage administrator can issue all commands that allocate and control storage resources for the server. An unrestricted storage administrator can issue commands that affect all existing storage pools as well as any storage pools that are defined in the future. An unrestricted storage administrator cannot define or delete storage pools. Using the GRANT AUTHORITY command with CLASSES=STORAGE and no STGPOOLS parameter upgrades a restricted storage administrator to an unrestricted storage administrator.

Operator

Specifies that you want to grant operator privilege to an administrator. An administrator with operator privilege can issue commands that control the immediate operation of the server and the availability of storage media.

Node

Specifies that you want to grant a node privilege to a user. A user with client node privilege can remotely access a web backup-archive client with an administrative user ID and password if they have been given owner authority or access authority. Access authority is the default for a node privilege class.
Attention: When you specify the node privilege class, you must also specify either the DOMAIN parameter or the NODE parameter, but not both.

AUTHority

Specifies the authority level of a user with node privilege. This parameter is optional.

If an administrator already has system or policy privilege to the policy domain to which the node belongs, this command will not change the administrator's privilege.

Possible authority levels are:

Access

Specifies that you want to grant client access authority to a user with the node privilege class. This is the default when CLASSES=NODE is specified. A user with client access authority can access a web backup-archive client and perform backup and restore actions on that client.
Attention: A user with client access authority cannot access that client from another system by using the -NODENAME or -VIRTUALNODENAME parameter.

A client node can set the REVOKEREMOTEACCESS option to restrict a user that has node privilege with client access authority from accessing a client workstation that is running a web client. This option does not apply to administrators with client owner authority, system privilege, or policy privilege to the policy domain to which the node belongs.

Owner

Specifies that you want to grant client owner authority to a user with the node privilege class. A user with client owner authority can access a web backup-archive client through the web client interface and also access their data from another client using the -NODENAME or -VIRTUALNODENAME parameter.

DOmains

Specifies that you want to grant to the administrator client access or client owner authority to all clients in the specified policy domain. You cannot use this parameter together with the NODE parameter.

NOde
Specifies that you want to grant the administrator client access or client owner authority to the node. You cannot use this parameter together with the DOMAIN parameter.

DOmains
When used with CLASSES=POLICY, specifies that you want to grant restricted policy privilege to an administrator.

Restricted policy privilege permits an administrator to issue a subset of the policy commands for the domains to which the administrator is authorized. You can use this parameter to grant additional policy domain authority to a restricted policy administrator. This parameter is optional. You can specify more than one policy domain by delimiting each policy domain name with a comma.

You can use wildcard characters to specify a name. Authority for all matching policy domains is granted.

STGpools
Specifies that you want to grant restricted storage privilege to an administrator. If the STGPOOLS parameter is specified, then CLASSES=STORAGE is optional.

Restricted storage privilege permits you to issue a subset of the storage commands for the storage pools to which the administrator is authorized. You can use this parameter to grant additional storage pool authority to a restricted storage administrator. This parameter is optional. You can specify more than one storage pool by delimiting each storage pool name with a comma.

You can use wildcard characters to specify a name. Authority for all matching storage pools is granted.

Example: Grant system privilege to an administrator

Grant system privilege to administrator Larry.

```
grant authority larry classes=system
```

Example: Grant access to additional policy domains

Specify additional policy domains that the restricted policy administrator CLAUDIA can manage.

```
grant authority claudia domains=employee_records,prog1
```

Example: Provide an administrator with unrestricted storage privilege and restricted policy privilege

Provide administrator TOM with unrestricted storage privilege and restricted policy privilege for the domains whose names start with EMP.

```
grant authority tom classes=storage domains=emp*
```

Example: Grant an administrator authority restricted to a specific node

Grant node privilege to user HELP so that help desk personnel can assist the client node LABCLIENT in backing up or restoring data without having other higher-level IBM Spectrum Protect privileges.

```
grant authority help classes=node node=labclient
```

Related commands

Table 1. Commands related to GRANT AUTHORITY

Command	Description
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
REVOKE AUTHORITY	Revokes one or more privilege classes or restricts access to policy domains and storage pools.

GRANT PROXYNODE (Grant proxy authority to a client node)

Use this command to grant proxy authority to a client node on the IBM Spectrum Protect™ server.

Target client nodes own the data and agent nodes act on behalf of the target nodes. When granted proxy authority to a target client node, an agent node can perform backup and restore operations for the target node. Data that the agent node stores on behalf of the target node is stored under the target node's name in server storage.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege

Syntax

```
>>-GRant PROXynode TArget--=--target_node_name------------------>

>--AGent--=--agent_node_name----------------------------------><
```

Parameters

TArget (Required)
: Specifies the name of the node that owns the data. Wildcard names cannot be used to specify the target node name.

AGent (Required)
: Specifies the name of the node performing operations for the target node. The agent node does not have to be in the same domain as the target node. Wildcard characters and comma-separated lists of node names are allowed.

Example: Grant proxy authority to a client node

Assume that MOE and JOE are agent nodes in a NAS cluster and are used to backup and restore shared NAS data. To create a proxy authority relationship for target node NASCLUSTER, issue the following command:

```
grant proxynode target=nascluster agent=moe,joe
```

Issue the following command on agent node MOE to back up NAS cluster data stored on the E: drive. The name of the target node is NASCLUSTER.

```
dsmc -asnode=nascluster incremental e:
```

Related commands

Table 1. Commands related to GRANT PROXYNODE

Command	Description
QUERY PROXYNODE	Display nodes with authority to act as proxy nodes.
REVOKE PROXYNODE	Revoke proxy authority from an agent node.

HALT (Shut down the server)

Use this command to shut down the server. The HALT command forces an abrupt shutdown, which cancels all the administrative and client node sessions even if they are not completed.

Any transactions in progress interrupted by the HALT command are rolled back when you restart the server. Use the HALT command only after the administrative and client node sessions are completed or canceled. To shut down the server without severely impacting administrative and client node sessions, perform the following steps:

1. Use the DISABLE SESSIONS command to prevent starting new client node sessions.
2. Use the QUERY SESSIONS command to identify any existing administrative and client node sessions.

3. Notify any existing administrative and client node sessions that you plan to shut down the server (you must do this outside of IBM Spectrum Protect™).
4. Use the CANCEL SESSIONS command to cancel any existing administrative or client node sessions.
5. Issue the HALT command to shut down the server and stop any administrative and client node sessions.

Tip:

The HALT command can be replicated using the ALIASHALT server option. Use the server option to define a term other than HALT that performs the same function. The HALT command retains its normal function however, the server option provides an additional method for issuing the HALT command. See ALIASHALT for additional information.

Privilege class

To issue this command, you must have system or operator privilege.

Syntax

```
>>-HALT-------------------------------------------------------><
```

Parameters

None.

Example: Shut down the server

Shut down the server, either from the server console or from an administrative client. All user activity stops immediately and no new activity can start.

```
halt
```

Related commands

Table 1. Commands related to HALT

Command	Description
CANCEL PROCESS	Cancels a background server process.
CANCEL SESSION	Cancels active sessions with the server.
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
QUERY PROCESS	Displays information about background processes.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.

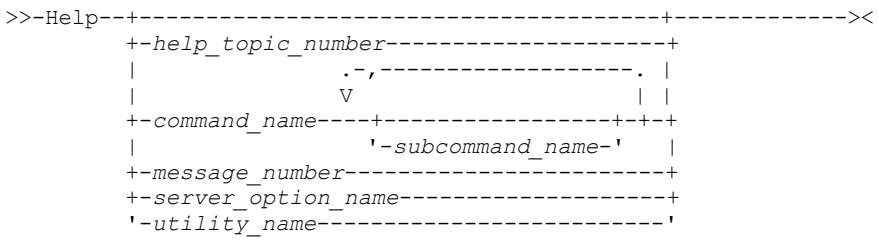
HELP (Get help on commands and error messages)

Use this command to display administrative commands and error messages. You can issue the command from an administrative command line client.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

help_topic_number
: Specifies the number of your selection from the help topics. This parameter is optional.
Topic numbers are displayed in the table of contents, for example:

```
3.0 Administrative commands
  ...
  3.13.10 DEFINE DEVCLASS (Define a device class)
      3.13.10.1 DEFINE DEVCLASS (Define a 3590 device class)
      3.13.10.2 DEFINE DEVCLASS (Define a 3592 device class)
      ...
```

The topic number for the command DEFINE DEVCLASS for a 3592 device class is 3.13.10.2.

command_name
: Specifies the name of the administrative command you want to display. This parameter is optional.

subcommand_name
: Specifies up to two of the subcommand names that are associated with the name of the administrative command that you want to display. This parameter is optional.

message_number
: Specifies the number of the message for which you want to display information. This parameter is optional. You can get help information about server messages (prefixed by ANR) and client messages (prefixed by ANE or ANS). Do not include the prefix and severity code when specifying an error message number.

server_option_name
: Specifies the name of the server option for which you want to display information. This parameter is optional.

utility_name
: Specifies the name of the server utility for which you want to display information. This parameter is optional.

Example: Display the help topics

Display the help topics for the command-line interface.

```
help
```

Partial output:

```
1.0 Administering the server from the command line
  1.1 Issuing commands from the administrative client
     1.1.1 Starting and stopping the administrative client
     1.1.2 Monitoring server activities from the administrative client
```

Example: Display a help topic by using the help topic number

Display help information by using the help topic number. The topic number for the command DEFINE DEVCLASS for a 3592 device class is 3.13.10.2.

```
help 3.13.10.2
```

Example: Display help for one command

Display help information about the REMOVE commands.

```
help remove
```

```
3.44 REMOVE commands
Use the REMOVE commands to remove an object.
The following is a list of REMOVE commands:
*  3.44.1, "REMOVE ADMIN (Delete an administrator)"
*  3.44.2, "REMOVE NODE (Delete a node or an associated machine node)"
```

Example: Display help for a specific error message

Display help information about the error message ANR2535E.

```
help 2535

ANR2535E  Command: The node node name cannot be removed or renamed
      because it has an associated data mover.
Explanation: You attempted to remove or rename a node that has an
associated data mover.
System action: The server does not remove or rename the node.
User response: To remove or rename the node, delete the associated data
mover and reissue the command.
```

Example: Display help for a specific option

Display the description, syntax, and an example for the COMMMETHOD server option.

```
help commmethod
```

Example: Display help for a specific utility

Display the description, syntax, and an example for the DSMSERV utility.

```
help dsmserv
```

IDENTIFY DUPLICATES (Identify duplicate data in a storage pool)

Use this command to start or stop processes that identify duplicate data in a storage pool. You can specify the number of duplicate-identification processes and their duration.

When you create a new storage pool for data deduplication, you can specify 0 - 50 duplicate-identification processes. IBM Spectrum Protect™ starts the specified number of duplicate-identification processes automatically when the server is started. If you do not stop them, they run indefinitely.

This command affects only server-side deduplication processing. In client-side data deduplication processing, duplicates are identified on the backup-archive client.

With the IDENTIFY DUPLICATES command, you can start more processes, stop some or all of the processes, and specify an amount of time that the change remains in effect. If you increased or decreased the number of duplicate-identification processes, you can use the IDENTIFY DUPLICATES command to reset the number of processes to the number that is specified in the storage pool definition.

If you did not specify any duplicate-identification processes in the storage pool definition, you can use the IDENTIFY DUPLICATES command to start and stop all processes manually.

This command starts or stops a background process or processes that you can cancel with the CANCEL PROCESS command. To display information about background processes, use the QUERY PROCESS command.

Important:

- You can also change the number of duplicate-identification processes by updating the storage pool definition by using the UPDATE STGPOOL command. However, when you update a storage pool definition, you cannot specify a duration. The processes that you specify in the storage pool definition run indefinitely, or until you issue the IDENTIFY DUPLICATES command, update the storage pool definition again, or cancel a process.

  Issuing the IDENTIFY DUPLICATES does not change the setting for the number of duplicate-identification processes in the storage pool definition.

- Duplicate-identification processes can be either active or idle. Processes that are deduplicating files are active. Processes that are waiting for files to deduplicate are idle. Processes remain idle until volumes with data to be deduplicated become

available. Processes stop only when canceled or when you change the number of duplicate-identification processes for the storage pool to a value less than what is specified. Before a duplicate-identification process stops, it must finish the file that it is deduplicating.

The output of the QUERY PROCESS command for a duplicate-identification process includes the total number of bytes and files that have been processed since the process first started. For example, if a duplicate-identification process processes four files, becomes idle, and then processes five more files, then the total number of files that are processed is nine.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-IDentify DUPlicates--stgpool_name----------------------------->

>--+----------------------+--+---------------------+--------><
   '-NUMPRocess--=--number-'  '-DURation--=--minutes-'
```

Parameters

stgpool_name (Required)
: Specifies the storage pool name in which duplicate data is to be identified. You can use wildcards.

NUMPRocess
: Specifies the number of duplicate-identification processes to run after the command completes. You can specify 0 - 50 processes. The value that you specify for this parameter overrides the value that you specified in the storage pool definition or the most recent value that was specified when you last issued this command. If you specify zero, all duplicate-identification processes stop.

  This parameter is optional. If you do not specify a value, the server starts or stops duplicate-identification processes so that the number of processes is the same as the number that is specified in the storage pool definition.

  For example, suppose that you define a new storage pool and specify two duplicate-identification processes. Later, you issue the IDENTIFY DUPLICATES command to increase the number of processes to four. When you issue the IDENTIFY DUPLICATES command again without specifying a value for the NUMPROCESS parameter, the server stops two duplicate-identification processes.

  If you specified 0 processes when you defined the storage pool definition and you issue IDENTIFY DUPLICATES without specifying a value for NUMPROCESS, any running duplicate-identification processes stop, and the server does not start any new processes.

  Remember: When you issue IDENTIFY DUPLICATES without specifying a value for NUMPROCESS, the DURATION parameter is not available. Duplicate-identification processes specified in the storage pool definition run indefinitely, or until you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.

  When the server stops a duplicate-identification process, the process completes the current physical file and then stops. As a result, it might take several minutes to reach the number of duplicate-identification processes that you specified as a value for this parameter.

DURation
: Specifies the maximum number of minutes (1 - 9999) that this command remains in effect. At the end of the specified time, the server starts or stops duplicate-identification processes so that the number of processes is the same as the number that is specified in the storage pool definition.

  This parameter is optional. If you do not specify a value, the processes that are running after the command is issued run indefinitely. They end only if you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.

  For example, if you define a storage pool with two duplicate-identification processes and you issue the IDENTIFY DUPLICATES command with `DURATION=60` and `NUMPROCESS=4`, the server starts two more duplicate-identification processes that run for 60 minutes. At the end of that time, two processes finish the files that they are working on and stop. The two processes that stop might not be the same two processes that started as a result of issuing this command.

The server stops idle processes first. If after stopping all idle processes, more processes need to be stopped, the server notifies active processes to stop.

When the server stops a duplicate-identification process, the process completes the current physical file and then stops. As a result, it might take several minutes to reach the amount of time that you specified as a value for this parameter.

Example: Controlling the number and duration of duplicate-identification processes

In this example, you specified three duplicate-identification processes in the storage pool definition. You use the IDENTIFY DUPLICATES command to change the number of processes and to specify the amount of time the change is to remain in effect.

Table 1. Controlling duplicate-identification processes manually

The storage pool definition specifies three duplicate-identification processes. Using the IDENTIFY DUPLICATES command, you specify...	**...and a duration of...**	**The result is...**
2 duplicate-identification processes	None specified	One duplicate-identification process finishes the file that it is working on, if any, and then stops. Two processes run indefinitely, or until you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.
	60 minutes	One duplicate-identification process finishes the file that it is working on, if any, and then stops. After 60 minutes, the server starts one process so that three are running.
4 duplicate-identification processes	None specified	The server starts one duplicate-identification process. Four processes run indefinitely, or until you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.
	60 minutes	The server starts one duplicate-identification process. At the end of 60 minutes, one process finishes the file that it is working on, if any, and then stops. The additional process started by this command might not be the one that stops when the duration has expired.
0 duplicate-identification processes	None specified	All duplicate-identification processes finish the files that they are working on, if any, and stop. This change lasts indefinitely, or until you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.
	60 minutes	All duplicate-identification processes finish the files that they are working on, if any, and stop. At the end of 60 minutes, the server starts three processes.
None specified	Not available	The number of duplicate-identification processes resets to the number of processes that are specified in the storage pool definition. This change lasts indefinitely, or until you reissue the IDENTIFY DUPLICATES command, update the storage pool definition, or cancel a process.

Example: Identify duplicates in a storage pool

Identify duplicates in a storage pool, STGPOOLA, using three duplicate-identification processes. Specify that this change is to remain in effect for 60 minutes.

```
identify duplicates stgpoola duration=60 numprocess=3
```

Related commands

Table 2. Commands related to IDENTIFY DUPLICATES

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY PROCESS	Displays information about background processes.
QUERY STGPOOL	Displays information about storage pools.
UPDATE STGPOOL	Changes the attributes of a storage pool.

IMPORT commands

Use the IMPORT commands to import information from export media to an IBM Spectrum Protect™ server.

Important: For commands that import administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the IMPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

- IMPORT ADMIN (Import administrator information)
- IMPORT NODE (Import client node information)
- IMPORT POLICY (Import policy information)
- IMPORT SERVER (Import server information)

IMPORT ADMIN (Import administrator information)

Use this command to import administrator and authority definitions for one or more administrators from export media to the IBM Spectrum Protect™ server.

Important: For commands that import administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the IMPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

You can use the QUERY ACTLOG command to view the status of the import operation.

You can also view this information from the server console.

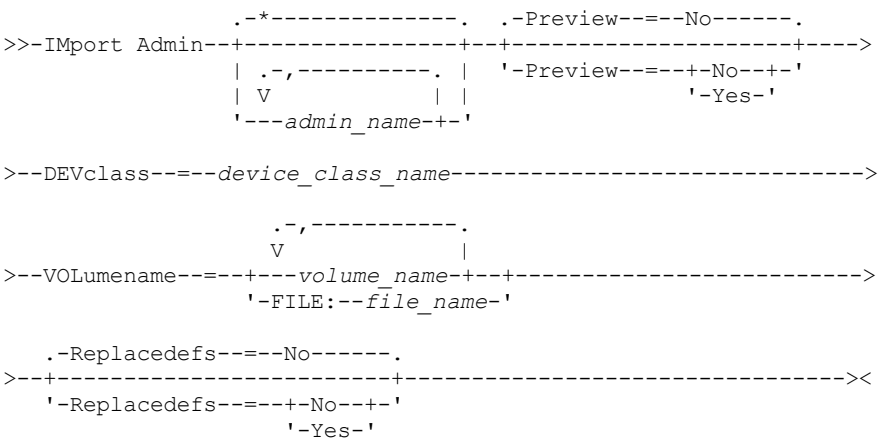
Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.
This command generates a background process that can be canceled with the CANCEL PROCESS command. If an IMPORT ADMIN background process is canceled, some of the data is already imported. To display information about background processes, use the QUERY PROCESS command.
Restriction:

- If target and source server levels are not compatible, the operation might not work.
- If the administrator definition that is being imported includes analyst authority, the administrator definition is imported but not the analyst authority. Analyst authority is not valid for servers at V6.1 or later.
- Importing data from a CENTERA device class is not supported. However, files that are being imported can be stored on a CENTERA storage device.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

admin_name
: Specifies the administrators for which you want to import information. This parameter is optional. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

Preview
: Specifies whether you want to preview the results of the import operation, without importing administrator information. This parameter is optional. The following parameters values are supported:

  No
  : Specifies that the information is to be imported.

  Yes
  : Specifies that the operation is previewed but not completed. Information about the number and types of objects that are imported, together with the number of bytes transferred, are reported to the server console and the activity log.

  The default value is NO. If you specify YES for the value, you must mount the export volumes.

DEVclass (Required)
: Specifies the device class from which import data is to be read.

  You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the import runs, IBM Spectrum Protect cancels lower priority operations, such as reclamation, to make a drive available.

VOLumename (Required)
: Specifies the volumes to be used for the import operation. Volumes must be imported in the same order as they were exported. The following parameter values are supported:

  volume_name
  : Specifies the volume name. To specify multiple volumes, separate names with commas and no intervening spaces.

  FILE:file_name
  : Specifies the name of a file that contains a list of volumes that are used for the imported data. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

  Use these naming conventions when you specify volumes that are associated with the following device types:

For this device	Specify
Tape	1 - 6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: AIX Linux /imdata/mt1. Windows d:\program files\tivoli\tsm\data1.dsm.

For this device	Specify
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1 - 6 alphanumeric characters.
SERVER	1 - 250 alphanumeric characters.

Replacedefs

Specifies whether to replace administrator definitions on the target server. The following parameter values are supported:

No

Specifies that definitions are not to be replaced.

Yes

Specifies that definitions are to be replaced.

The default value is NO.

Example: Import administrator information from specific tape volumes

From the server, import the information for all defined administrators from tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class. Issue the command:

```
import admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Example: Import administrator information from tape volumes listed in a file

From the server, import the information for all defined administrators from tape volumes that are listed in the following file:

- AIX Linux TAPEVOL
- Windows TAPEVOL.DATA

This file contains these lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that these tape volumes be read by a device that is assigned to the MENU1 device class. Issue the command:

AIX Linux

```
import admin devclass=menu1 volumenames=file:tapevol
```

Windows

```
import admin devclass=menu1 volumenames=file:tapevol.data
```

Related commands

Table 1. Commands related to IMPORT ADMIN

Command	Description
CANCEL PROCESS	Cancels a background server process.
EXPORT ADMIN	Copies administrative information to external media or directly to another server.
IMPORT NODE	Restores client node information from external media.
IMPORT POLICY	Restores policy information from external media.
IMPORT SERVER	Restores all or part of the server from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

IMPORT NODE (Import client node information)

Use this command to import client node definitions from a server or sequential media to a target IBM Spectrum Protect™ server.

Important: For commands that import administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the IMPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

If you specify a domain on the source server and if that policy domain also exists on the target server, the imported nodes get associated with that same policy domain on the target server. Otherwise, imported nodes are associated with the STANDARD policy domain on the target server.

IBM Spectrum Protect servers with retention protection enabled do not allow import operations.

Restrictions:

1. If target and source server levels are not compatible, the operation might not work.
2. Importing data from a CENTERA device class is not supported. However, files that are being imported can be stored on a CENTERA storage device.
3. If you use an LDAP directory server to authenticate passwords, any target servers must be configured for LDAP passwords. Data that is imported from a node that authenticates with an LDAP directory server is inaccessible if the target server is not properly configured. If your target server is not configured, imported data from an LDAP node can still go there. But the target server must be configured to use LDAP in order for you to access the imported data.
4. If target and source server levels are not compatible, the operation might not work.
5. You cannot use a CENTERA device class as the target medium for an export command, or as the source medium for an import command.
6. Incrementally exporting/importing the following types of client data to another IBM Spectrum Protect server is not supported:
   - VMWare backups where full plus incremental backups need to be periodically, incrementally transferred to another server.
   - Backups groups where full plus differential backups need to be periodically, incrementally transferred to another server.
   - Windows Windows System State data that is periodically, incrementally transferred to another server.

   Full export/import of this data to a new file system on the target is supported by exporting the entire filespace that contains the data. In other words, the export must not use the *FILEDATA=ALLACTIVE*, *FROMDATE*, *TODATE*, or *MERGEFILESPACES* options.

   The best practice for incrementally transferring this type of data between two servers is to use Node Replication.

You can use the QUERY ACTLOG command to view the status of the import operation. You can also view this information from the server console.

This command generates a background process that can be canceled with the CANCEL PROCESS command. If an IMPORT NODE background process is canceled, some of the data might already be imported. To display information about background processes, use the QUERY PROCESS command.

For a server that has clients with support for Unicode, you can get the server to convert the file space name that you enter, or use the following parameters:

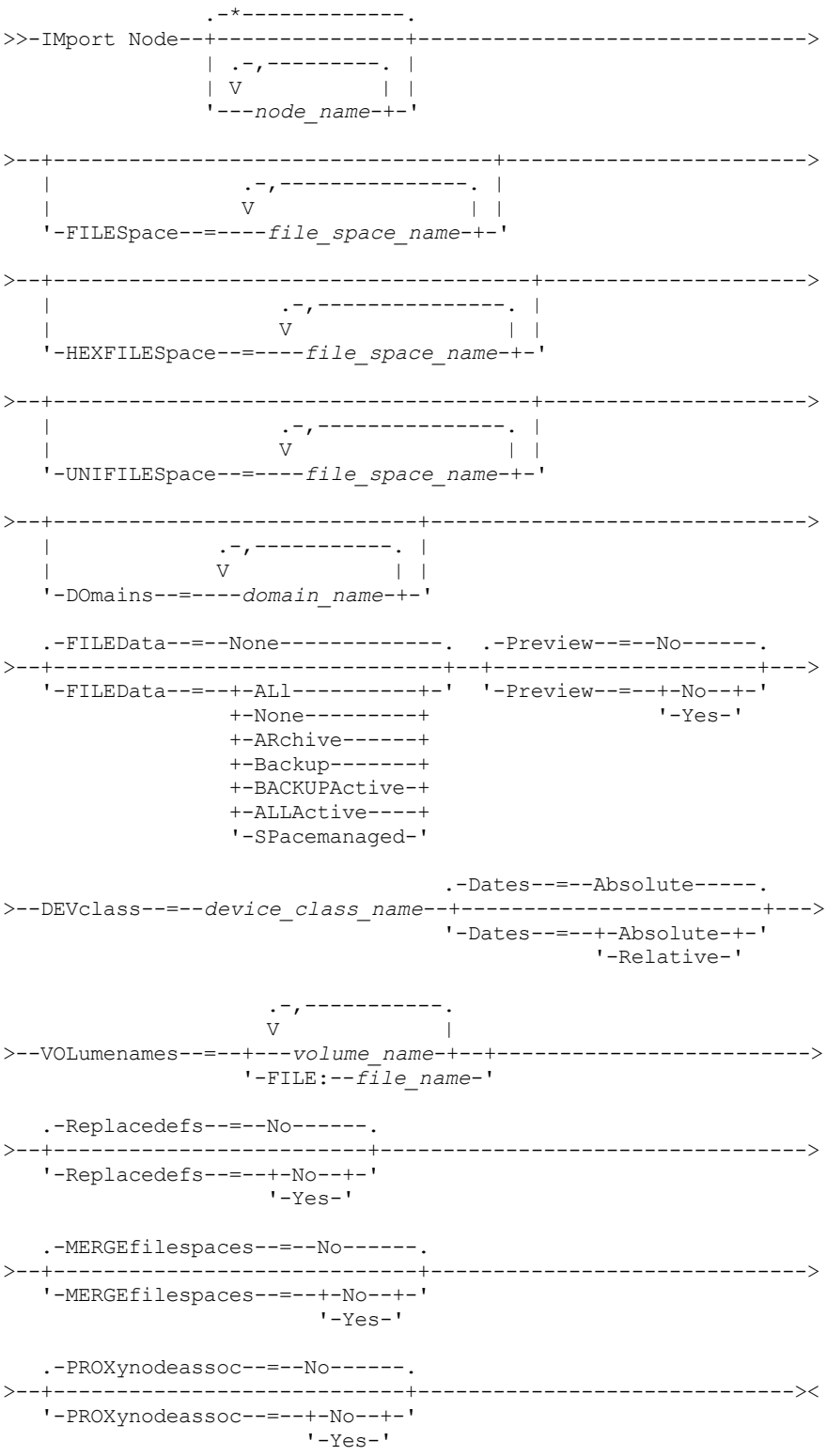
- HEXFILESPACE
- UNIFILESPACE

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

node_name
: Specifies the client nodes for which you want to import information. This parameter is optional.

  Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. All matching nodes are included in the list.

FILESpace

Specifies file space names for which you want to import information. This parameter is optional. The default is all file spaces.

Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

Important:

1. Existing file spaces are not replaced. New file spaces are created when identical names are encountered. However, this new name might match an existing name on the client node, which can have file spaces that are not yet backed up to the server.
2. This parameter is only specified for non-Unicode file spaces. To import all file spaces that are both Unicode and non-Unicode, use the FILEDATA=ALL parameter without the FILESPACE and UNIFILESPACE parameters.

DOmains
Specifies the policy domains from which to import node information. These domains must be included in the data that was exported. This parameter is optional. The default is all domains that were exported.

Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify a name.

FILEData
Specifies the type of files that can be imported for all nodes that are specified and found on the export media. This parameter is optional. The default value is NONE.

If you are importing from sequential media, the device class that is used by the file data is determined by the device class for the storage pool. If it is the same device class that is specified in this command, two drives are needed to import the node information. The mount limit for the device class must be at least 2.

The following descriptions mention *active* and *inactive* backup file copies. An active backup file copy is the most recent backup copy for a file that still exists on the client workstation. All other backup file copies are called inactive copies. The parameter supports the following values:

ALl
: The server imports all backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client. The file spaces that are included are both Unicode and non-Unicode.

None
: Only node definitions are imported. The server does not import any files.

ARchive
: The server imports only archived files.

Backup
: The server imports only backup versions, whether active or inactive.

BACKUPActive
: The server imports only active backup versions. These active backup versions are the active versions in the IBM Spectrum Protect database at the time that the IMPORT command is issued.

ALLActive
: The server imports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client. The active backup versions are the active versions in the IBM Spectrum Protect database at the time that the IMPORT command is issued.

SPacemanaged
: The server imports only files that were migrated by an IBM Spectrum Protect for Space Management client.

Preview
Specifies whether to preview the results of the import operation, without importing information. The PREVIEW=YES option requires that you mount the export volumes. The following values are supported:

No
: Specifies that the node information is to be imported.

Yes
: Specifies that you want to preview the results of the import operation, without importing files. Information is reported to the server console and the activity log.

This parameter is optional. The default value is NO.

DEVclass (Required)

Specifies the device class from which import data is to be read. You cannot specify the DISK, NAS, or CENTERA device classes.

If all drives for the device class are busy when the import runs, the server cancels lower priority operations, such as identify duplicates, to make a drive available.

Dates

Specifies whether the dates for the file copies are set as the same date when the files were exported, or is adjusted to the import date.
This parameter supports the following values:

Absolute
: The dates for file copies are set to the values specified when the files were exported.

Relative
: The dates for file copies are adjusted to the import date.

The default value is ABSOLUTE.

If the export media is idle for some time after export, for example; if it is sitting on a shelf for six months, the original backup, or archive dates might be old enough to trigger the file copies to expire immediately when the data is imported into a server. The RELATIVE specification for this value adjusts for time that is elapsed since export so that the file copies are not immediately expired.

For example, assume that an export tape contains an archive file copy that was archived five days before the export operation. If the media is saved for six months and then imported, the archive file look like it is inserted six months and five days ago by default, the (DATES=ABSOLUTE) and might expire immediately depending on the retention value that is specified in the file's management class. Specifying DATES=RELATIVE results in resetting the archive date for the file to five days ago during import. The DATES=RELATIVE parameter thus adjusts file backup and archive dates for the time that elapsed since the export operation occurred.

VOLumenames (Required)

Specifies the volumes to be used for the import operation. Volumes must be imported in the same order as they were exported. The parameter supports the following values:

volume_name
: Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

FILE:file_name
: Specifies the name of a file that contains a list of volumes that are used for the imported data. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when you specify volumes that are associated with the following device types:

For this device	**Specify**
Tape	1 - 6 alphanumeric characters.
FILE	AIX Linux Any fully qualified file name string. An example is /imdata/mt1. Windows Any fully qualified file name string. For example, d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1 - 6 alphanumeric characters.
SERVER	1 - 250 alphanumeric characters.

Replacedefs

Specifies whether to replace definitions on the target server. The default value is NO. The parameter supports the following values:

No
: Objects are not to be replaced.

Yes
: Objects are to be replaced.

HEXFILESpace

Specifies the hexadecimal representation of the file space names in UTF-8 format. Separate multiple names with commas and no intervening spaces. This parameter is optional.

To view the hexadecimal representation of a file space name, you can use the QUERY FILESPACE command with FORMAT=DETAILED.

UNIFILESpace
: Specifies that the file spaces that are known to the server are Unicode enabled. The server converts the names that you enter from the server code page to the UTF-8 code page to find the file spaces to import. The success of the conversion depends on the actual characters in the name and the server's code page. Separate multiple names with commas and no intervening spaces. A wildcard character can be used to specify a name. This parameter is optional.

MERGEfilespaces
: Specifies whether IBM Spectrum Protect merges client files into existing file spaces on the target server (if they exist), or if IBM Spectrum Protect generates new file space names. The default is NO.

  Valid values are:

  Yes
  : Specifies that imported data on the target server is merged with the existing file space, if a file space with the same name exists on the target server.

  No
  : Specifies that IBM Spectrum Protect generates a new file space name for imported data on the target server if file spaces with the same name exists.

PROXynodeassoc
: Specifies whether proxy node associations are imported. This parameter is optional. The default value is NO.

Example: Import client node information from tapes

From the server, import client node information from tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class.

```
import node devclass=menu1 volumenames=tape01,tape02,tape03
```

Example: Import client node information from tapes listed in a file

AIX Linux From the server, import client node information from tape volumes that are listed in a file named TAPEVOL.

Windows From the server, import client node information from tape volumes that are listed in a file named TAPEVOL.DATA.

This file contains these lines:

```
TAPE01
TAPE02
TAPE03
```

Specify that these tape volumes be read by a device that is assigned to the MENU1 device class. AIX Linux

```
import node devclass=menu1 volumenames=file:tapevol
```

Windows

```
import node devclass=menu1 volumenames=file:tapevol.data
```

Example: Import the active backup for a client node

From the server, import the active backup versions of file data for client node JOE from tape volume TAPE01. The file space is Unicode.

```
import node joe unifilespace=\\joe\c$ filedata=backupactive devclass=menu1
    volumenames=tape01
```

Related commands

Table 1. Commands related to IMPORT NODE

Command	Description
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.

Command	Description
EXPORT NODE	Copies client node information to external media or directly to another server.
IMPORT ADMIN	Restores administrative information from external media.
IMPORT POLICY	Restores policy information from external media.
IMPORT SERVER	Restores all or part of the server from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

IMPORT POLICY (Import policy information)

Use this command to import policy domain information from sequential export media to the IBM Spectrum Protect™ server. IBM Spectrum Protect servers with retention protection enabled do not allow import operations.

IBM Spectrum Protect client data can be moved between servers with export and import processing, if the same removable media type is supported on both platforms.

Restriction:

1. If target and source server levels are not compatible, the import operation might not work.
2. Importing data from a CENTERA device class is not supported. However, files that are imported can be stored on a CENTERA storage device.

You can use the QUERY ACTLOG command to view the status of the import operation. You can also view this information from the server console.

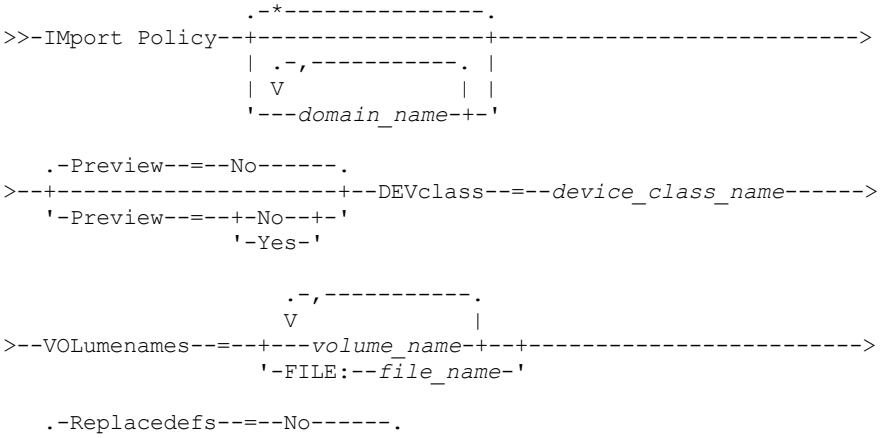
This command generates a background process that can be canceled with the CANCEL PROCESS command. If an IMPORT POLICY background process is canceled, some of the data is already imported. To display information about background processes, use the QUERY PROCESS command.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

Privilege class

To issue this command, you must have system privilege.

Syntax



```
>--+-------------------------+--------------------------------><
   '-Replacedefs--=--+-No--+-'
                     '-Yes-'
```

Parameters

domain_name
: Specifies the policy domains for which information is to be imported. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. The default (*) is all policy.

Preview
: Specifies whether you want to preview the results of the import operation without importing information.This parameter supports the following values:

  No
  : Specifies that the information is to be imported.

  Yes
  : Specifies that the operation is previewed but not completed. Information is reported to the server console and the activity log.

  The PREVIEW=YES option requires that you mount the export volumes. This parameter is optional. The default value is NO.

DEVclass (Required)
: Specifies the device class from which import data is to be read. You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the import runs, IBM Spectrum Protect cancels lower priority operations, such as reclamation, to make a drive available.

VOLumenames (Required)
: Specifies the volumes to be used for the import operation. Volumes must be imported in the same order as they were exported. This parameter supports the following values:

  volume_name
  : Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

  FILE:file_name
  : Specifies the name of a file that contains a list of volumes. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

  Use these naming conventions when you specify volumes that are associated with the following device types:

For this device	Specify
Tape	1 - 6 alphanumeric characters.
FILE	Any fully qualified file name string. For example: • AIX Linux /imdata/mt1 • Windows d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1 - 6 alphanumeric characters.
SERVER	1 - 250 alphanumeric characters.

Replacedefs
: Specifies whether to replace policy definitions on the target server. This parameter supports the following values:

  Yes
  : Specifies that objects are to be replaced by the imported objects.

  No
  : Specifies that objects are not to be replaced by imported objects.

  The default value is NO.

Example: Import policy information from specific tape volumes

From the server, import the information for all defined policies from tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class.

```
import policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Example: Import policy information from tape volumes listed in a file

From the server, import the information for all defined policies from tape volumes that are listed in a file that is named thus:

- AIX Linux TAPEVOL
- TAPEVOL.DATA

Specify that these tape volumes be read by a device that is assigned to the MENU1 device class. The file contains the following lines:

```
TAPE01
TAPE02
TAPE03
```

AIX Linux

```
import policy devclass=menu1 volumenames=file:tapevol
```

Windows

```
import policy devclass=menu1 volumenames=file:tapevol.data
```

Related commands

Table 1. Commands related to IMPORT POLICY

Command	Description
CANCEL PROCESS	Cancels a background server process.
EXPORT POLICY	Copies policy information to external media or directly to another server.
IMPORT ADMIN	Restores administrative information from external media.
IMPORT NODE	Restores client node information from external media.
IMPORT SERVER	Restores all or part of the server from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

IMPORT SERVER (Import server information)

Use this command to copy all or part of the server control information and specified client file data from export media to the IBM Spectrum Protect™ server.

Important: For commands that import administrators or nodes, you must consider the method of authentication. The IBM Spectrum Protect server cannot export or import passwords for nodes or administrators that are authenticating with LDAP directory servers. If the current authentication method uses an LDAP directory server and the password is not already synchronized by that server, you must update the password. After issuing the IMPORT command, set the password by issuing the UPDATE ADMIN or UPDATE NODE command.

IBM Spectrum Protect servers with retention protection enabled do not allow import operations.

Restrictions:

- If target and source server levels are not compatible, the operation might not work.
- Importing data from a CENTERA device class is not supported. However, files that are imported can be stored on a CENTERA storage device.
- If you use an LDAP directory server to authenticate passwords, any target servers must be configured for LDAP passwords. Server data that is exported from a node that authenticates with an LDAP directory server is inaccessible if the target server

is not properly configured. If your target server is not configured, exported data from an LDAP node can still go there. But the target server must be configured to use LDAP in order for you to access the data.

- Incrementally exporting or importing the following types of client data to another IBM Spectrum Protect server is not supported:
  - VMware backups where full plus incremental backups need to be periodically, incrementally transferred to another server
  - Backups groups where full plus differential backups must be periodically, incrementally transferred to another server
  - Windows System State data that is periodically, incrementally transferred to another server

  Full export or import of this data to a new file system on the target is supported by exporting the entire file space that contains the data. The export must not use the FILEDATA=ALLACTIVE, FROMDATE, TODATE, or MERGEFILESPACES parameters.

  Using node replication to incrementally transfer this type of client data between two servers is optimal.

You can also initiate an import of server information and client file data directly from the originating server. For more information, see the EXPORT commands.

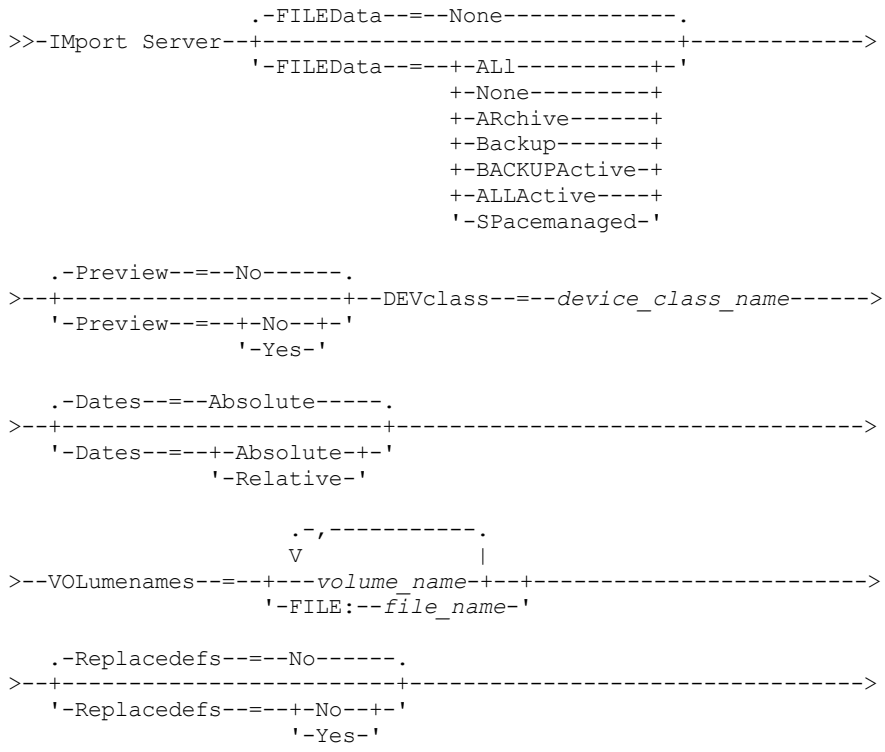
This command generates a background process that can be canceled with the CANCEL PROCESS command. If an IMPORT SERVER background process is canceled, some of the data is already imported. To display information about background processes, use the QUERY PROCESS command.

Limitation: The IBM Spectrum Protect server does not convert code pages during export, import, and node replication operations. If servers are running in different locales, some information in databases or system output might become unreadable. Invalid characters might be displayed, for example, in the contact information for the administrator and client nodes, and in descriptions of policy domains. Any field that is stored in the server character set and that includes extended ASCII characters can be affected. To resolve the issue after the import or node replication operation, update the fields with the appropriate UPDATE commands. This server limitation does not affect client data. Any client data that was exported, imported, or replicated can be restored, retrieved, and recalled.

Privilege class

To issue this command, you must have system privilege.

Syntax



```
   .-MERGEfilespaces--=--No------.
>--+----------------------------+----------------------------->
   '-MERGEfilespaces--=--+-No--+-'
                         '-Yes-'

   .-PROXynodeassoc--=--No------.
>--+----------------------------+----------------------------><
   '-PROXynodeassoc--=--+-No--+-'
                        '-Yes-'
```

Parameters

FILEData
: Specifies the type of files that can be imported for all nodes that are defined to the server. This parameter is optional. The default value is NONE.

  The device class that is used to access the file data is determined by the device class for the storage pool. If it is the same device class that is specified in this command, two drives are needed to import information. The mount limit for the device class must be set to at least 2.

  The following descriptions mention active and inactive backup file copies. An active backup file copy is the most recent backup copy for a file that still exists on the client workstation. All other file copies are called inactive copies. This parameter supports the following values:

  ALl
  : IBM Spectrum Protect imports all backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client.

  None
  : IBM Spectrum Protect does not import files, only node definitions.

  ARchive
  : IBM Spectrum Protect imports only archived files.

  Backup
  : IBM Spectrum Protect imports only backup versions, whether the versions are active or inactive.

  BACKUPActive
  : IBM Spectrum Protect imports only active backup versions. These active backup versions are the active versions in the IBM Spectrum Protect database at the time that the IMPORT command is issued.

  ALLActive
  : IBM Spectrum Protect imports all active backup versions of files, all archived files, and all files that were migrated by an IBM Spectrum Protect for Space Management client. The active backup versions are the active versions in the IBM Spectrum Protect database at the time that the IMPORT command is issued.

  SPacemanaged
  : IBM Spectrum Protect imports only files that were migrated by an IBM Spectrum Protect for Space Management client.

Preview
: Specifies whether to preview the results of the import operation, without importing information. This parameter supports the following values:

  No
  : Specifies that the server information is to be imported.

  Yes
  : Specifies that the operation is previewed but not completed. Information is transferred to the server console and the activity log.

  This parameter is optional. The default value is NO. If the PREVIEW=YES option is specified, you must mount the export volumes.

DEVclass (Required)
: Specifies the device class from which import data is to be read. You cannot specify the DISK, NAS, or CENTERA device classes.

  If all drives for the device class are busy when the import runs, IBM Spectrum Protect cancels lower priority operations, such as reclamation, to make a drive available.

Dates

Specifies whether the dates for the file copies are set as the same date when the files were exported, or is adjusted to the import date.

If the import media is idle for some time after export, for example; if it is sitting on a shelf for six months, the original backup, or archive dates might be old enough to trigger the file copies to expire immediately when the data is imported into a server. The RELATIVE specification for this value adjusts for time that is elapsed since export so that the file copies are not immediately expired.

For example, assume that an import tape contains an archive file copy that was archived five days before the export operation. If the export media are saved for six months and then imported, the archive file looks like it is inserted six months and five days ago by default (DATES=ABSOLUTE) and might expire immediately depending upon the retention value that is specified in the file's management class. Specifying DATES=RELATIVE results in resetting the archive date for the file to five days ago during import. DATES=RELATIVE parameter thus adjusts file backup and archive dates for the time that elapsed since the export operation occurred.

This parameter supports the following values:

Absolute
: The dates for file copies are set to the values specified when the files were exported.

Relative
: The date for file copies are adjusted to the date of import.

The default value is ABSOLUTE.

VOLumenames (Required)
: Specifies the volumes to be used for the import operation. Volumes must be imported in the same order as they were exported. This parameter supports the following values:

volume_name
: Specifies the volume name. To specify multiple volumes, separate the names with commas and no intervening spaces.

FILE:file_name
: Specifies the name of a file that contains a list of volumes that are used for the imported data. In the file, each volume name must be on a separate line. Blank and comment lines that begin with an asterisk are ignored.

Use these naming conventions when you specify volumes that are associated with the following device types:

For this device	Specify
Tape	1 - 6 alphanumeric characters.
FILE	AIX Linux Any fully qualified volume or file name string. An example is /imdata/mt1. Windows Any fully qualified volume or file name string. For example, d:\program files\tivoli\tsm\data1.dsm.
AIX Linux Windows REMOVABLEFILE	AIX Linux Windows 1 - 6 alphanumeric characters.
SERVER	1 - 250 alphanumeric characters.

Replacedefs
: Specifies whether to replace objects on the server. Existing file spaces are not replaced. New file spaces are created when identical names are encountered. This parameter supports the following values:

No
: Specifies that objects are not to be replaced by imported objects.

Yes
: Specifies that objects are to be replaced by the imported objects.

The default value is NO.

MERGEfilespaces
: Specifies whether IBM Spectrum Protect merges client files into existing file spaces on the target server (if they exist), or if IBM Spectrum Protect generates new file space names. You cannot merge non-Unicode and Unicode file spaces together. This parameter supports the following values:

No

Specifies that IBM Spectrum Protect generates a new file space name for imported data on the target server if file spaces with the same name exist.

Yes

Specifies that imported data on the target server is merged with the existing file space, if a file space with the same name exists on the target server.

The default is NO.

PROXynodeassoc

Specifies whether proxy node associations are imported. This parameter is optional. The default value is NO.

Example: Import the information for all defined servers from specific tapes

From the server, import the information for all defined servers from tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03
```

AIX Linux

Example: Import information for all defined servers from specific tapes and specify files are merged into existing file spaces

From the server, import the information for all defined servers from tape volumes TAPE01, TAPE02, and TAPE03. Specify that these tape volumes be read by a device that is assigned to the MENU1 device class and that client files be merged into file spaces on the target server if file spaces of the same names exist.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03 mergefilespaces=yes
```

Example: Import information for all defined servers from tapes listed in a file

From the server, import the information for all defined servers from tape volumes that are listed in a file named TAPEVOL. Specify that the tape volumes are read by a device that is assigned to the MENU1 device class. The input file contains these lines:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol
```

Windows

Example: Import information for all defined servers from tapes listed in a file

From the server, import the information for all defined servers from tape volumes that are listed in a file named TAPEVOL.DATA. Specify that the tape volumes are read by a device that is assigned to the MENU1 device class. The input file contains these lines:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol.data
```

Related commands

Table 1. Commands related to IMPORT SERVER

Command	Description
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT ADMIN	Restores administrative information from external media.
IMPORT NODE	Restores client node information from external media.

Command	Description
IMPORT POLICY	Restores policy information from external media.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY PROCESS	Displays information about background processes.

INSERT MACHINE (Insert machine characteristics information or recovery instructions)

Use this command to add client machine characteristics or recovery instructions to existing machine information in the database.

You can write a program to read files containing the information and generate the appropriate INSERT MACHINE commands.

You can use QUERY commands to retrieve the information if a disaster occurs.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-INsert MAchine--machine_name--sequence_number---------------->

>--+-CHaracteristics--=--text------+--------------------------><
   '-RECOVERYInstructions--=--text-'
```

Parameters

machine_name (Required)
: Specifies the name of the client machine.

sequence_number (Required)
: Specifies the sequence number for the line of text in the database.

CHaracteristics
: Specifies machine characteristics information. You must specify the characteristics or recovery instructions, but not both. Enclose the text in quotation marks if it contains blank characters. The text can be up to 1024 characters.

RECOVERYInstructions
: Specifies recovery instructions. You must specify the characteristics or recovery instructions, but not both. Enclose the text in quotation marks if it contains blank characters. The text can be up to 1024 characters.

Example: Update a machine's information

For the machine DISTRICT5, insert this characteristics text on line 1: "Machine owner is Mary Smith".

```
insert machine district5 1
characteristics="Machine owner is Mary Smith"
```

Related commands

Table 1. Commands related to INSERT MACHINE

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
DELETE MACHINE	Deletes a machine.
QUERY MACHINE	Displays information about machines.

Related information:

Specifying information about your server and client node machines

ISSUE MESSAGE (Issue a message from a server script)

Use this command with return code processing in a script to issue a message from a server script to determine where the problem is with a command in the script.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-ISSUE MESSAGE--message_severity--message_text--------------><
```

Parameters

message_severity (Required)
Specifies the severity of the message. The message severity indicators are:

I
Information. ANR1496I is displayed in the message text.

W
Warning. ANR1497W is displayed in the message text.

E
Error. ANR1498E is displayed in the message text.

S
Severe. ANR1499S is displayed in the message text.

message_text (Required)
Specifies the description of the message.

Example: Issue a message from a server script

Assume you have a script called backupscript that quiesces a client's database, takes a backup of that database, and then restarts the client's database. For illustration, your script results in a non-zero return code. Use the ISSUE MESSAGE command with the message severity and message text. The following is an example of a server script that calls backupscript on the client machine and issues messages based on the return code from backupscript.

```
issue message i "Starting backup"
define clientaction nodename action=command objects="c:\backupscript" wait=yes
if (101) goto qfail
if (102) goto qwarn
if (103) goto backupf
if (104) goto restartf
issue message i "Backup of database complete"
exit
qfail: issue message e "Quiesce of database failed"
exit
qwarn: issue message w "Quiesce of database failed, taking fuzzy backup"

exit
backupf: issue message e "Backup of database failed"
exit
restartf: issue message s "Database restart failed"
exit
```

Command

```
issue message e "quiesce of database failed"
```

Related commands

Table 1. Commands related to ISSUE MESSAGE

Command	Description

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

LABEL LIBVOLUME (Label a library volume)

Use this command to label tape volumes or, in an automated library, to label the volumes automatically as they are checked in. With this command, the server uses the full-length label with which the volumes are often prelabeled.

Restriction: Use this command only for MANUAL, SCSI, ACSLS, and 349X libraries. The command processing does not wait for a drive to become available, even if the drive is only in the IDLE state. If necessary, you can make a library drive available by issuing the DISMOUNT VOLUME command to dismount the volume in that particular drive. When the library drive becomes available, you can reissue the LABEL LIBVOLUME command.
For detailed and current drive and library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

AIX Linux

To use the LABEL LIBVOLUME command, at least one drive must exist that is not in use by another IBM Spectrum Protect™ process. This includes idle volumes that are mounted. If necessary, use the DISMOUNT VOLUME command to dismount the idle volume to make that drive available.

By default, the LABEL LIBVOLUME command does not overwrite an existing label. However, if you want to overwrite an existing label, you can specify the `OVERWRITE=YES` option.

Attention:

- By overwriting a volume label, you destroy all data on the volume. Use caution when you overwrite volume labels to avoid deleting valid data.
- The labels on VolSafe volumes can be overwritten only once. Therefore, use the LABEL LIBVOLUME command only once for VolSafe volumes. You can guard against overwriting the label by using the `OVERWRITE=NO` option with the LABEL LIBVOLUME command.

When you use the LABEL LIBVOLUME command, you can identify the volumes to be labeled in one of the following ways:

- Explicitly name one volume.
- Enter a range of volumes by using the VOLRANGE parameter.
- Use the VOLLIST parameter to specify a file that contains a list of volume names or to explicitly name one or more volumes.

For automated libraries, you are prompted to insert the volume in the entry/exit slot of the library.

When virtual input/output (VIO) is enabled, volumes that are in the I/O station are no longer in entry/exit ports. To ensure that the volumes can be processed, move them from the I/O station to VIO slots. If no I/O convenience station is available, insert the volume into an empty slot.

For manual libraries, you are prompted to load the volume directly into a drive.

Tip: To automatically label tape volumes, you can use the AUTOLABEL parameter on the DEFINE LIBRARY and UPDATE LIBRARY commands. By using the AUTOLABEL parameter, you eliminate the need to pre-label a set of tapes. This method is more efficient than using the LABEL LIBVOLUME command, which requires you to mount volumes separately. If you use the AUTOLABEL parameter with a SCSI library, you must check in tapes by specifying `CHECKLABEL=BARCODE` on the CHECKIN LIBVOLUME command. The AUTOLABEL parameter defaults to YES for all non-SCSI libraries and to NO for SCSI libraries.
Windows

To label volumes with the LABEL LIBVOLUME command, specify the CHECKIN parameter.

To automatically label tape volumes in SCSI-type libraries, use the AUTOLABEL parameter on the DEFINE LIBRARY and UPDATE LIBRARY commands. By using this parameter, you eliminate the need to pre-label a set of tapes. This method is also more efficient than using the LABEL LIBVOLUME command, which requires you to mount volumes separately. If you use the AUTOLABEL parameter, you must check in tapes by specifying CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

A label cannot include embedded blanks or periods and must be valid when used as a file name on the media.

You must label CD-ROM, Zip, or Jaz volumes with the device utilities from the manufacturer or the Windows utilities. IBM Spectrum Protect does not provide utilities to format or label these media types. The operating system utilities include the Disk Administrator program (a graphical user interface) and the label command.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax for a manual library

```
>>-LABEl LIBVolume--library_name------volume_name--------------->

   .-OVERWRITE--=--No------.  .-WAITTime--=--60----.
>--+-----------------------+--+--------------------+----------><
   '-OVERWRITE--=--+-No--+-'  '-WAITTime--=--value-'
                   '-Yes-'
```

Syntax for a SCSI library

```
>>-LABEl LIBVolume--library_name------------------------------->

>----+-volume_name-------------------------------------------------------+---->
     '-SEARCH--=--+-Yes--| A |--+--LABELSource--=--+-Barcode--------+-'
                  '-Bulk--| A |-'                 +-Prompt---------+
                                                  '-Vollist--| B |-'

                                .-OVERWRITE--=--No------.
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                    '-Yes-'

   .-WAITTime--=--60----.
>--+--------------------+-------------------------------------><
   '-WAITTime--=--value-'

A (SEARCH=Yes, SEARCH=Bulk)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |                .-,-----------.              |
   |                V             |              |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'

B (LABELSource=Vollist)

                 .-,-----------.
                 V             |
|--VOLList--=--+---volume_name-+--+----------------------------|
               '-FILE:--file_name-'
```

Syntax for a 349X library

```
>>-LABEl LIBVolume--library_name------------------------------->

>----+-volume_name--------------+----------------------------->
     '-SEARCH--=--Yes----| A |---'

                                .-OVERWRITE--=--No------.
```

```
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                   '-Yes-'

   .-WAITTime--=--60----.
>--+--------------------+-------------------------------------><
   '-WAITTime--=--value-'

A (SEARCH=Yes)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.               |
   |               V             |               |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Syntax for an ACSLS library

```
>>-LABel LIBVolume--library_name------------------------------->

>----+-volume_name---------------+------------------------------>
     '-SEARCH--=--Yes----| A |---'

                                .-OVERWRITE--=--No------.
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                   '-Yes-'

   .-WAITTime--=--60----.
>--+--------------------+-------------------------------------><
   '-WAITTime--=--value-'

A (SEARCH=Yes)

|--+-VOLRange--=----volume_name1,volume_name2---+---------------|
   |               .-,-----------.               |
   |               V             |               |
   '-VOLList--=--+---volume_name-+--+-----------'
                 '-FILE:--file_name-'
```

Parameters

library_name (Required)
: Specifies the name of the library that contains the storage volume.

volume_name
: Specifies the name of the volume to be labeled.

  - For SCSI libraries: The server requests that the volume is inserted into a slot in the library or, if available, into an entry/exit port. The server identifies a slot by the slot's element address. If you are labeling a volume in a SCSI library with multiple entry/exit ports, the volume in the lowest numbered slot is labeled.
    Warning: If you specify a volume name, the name you specify overrides the label that is printed on the cartridge.
  - For MANUAL libraries: The server requests that the volume is inserted into a drive.
  - For 349X libraries: The volume might already be in the library, or you might be prompted to put it into the I/O station.

  Remember: If the specified volume name is already defined in a storage pool or in a volume history file, the volume is not labeled, and a message is displayed.

CHECKIN
: Specifies whether the server checks in the volume. This parameter is optional. The following are possible values:

  SCRatch
  : Specifies that the server checks in the volumes and adds them to the library's scratch pool. If a volume has an entry in volume history, you cannot check it in as a scratch volume.

  PRIvate
  : Specifies that the server checks in the volumes and designates them as private. Private volumes are available only when you request them by name.

If you do not specify a value for this parameter, the command labels the volume, but does not check it in. If you do not specify a value for this parameter and you want to check in the volume, you must issue the CHECKIN LIBVOLUME command.

SEARCH

Specifies that the server searches the library for usable volumes to label. This parameter applies to SCSI, 349X, and ACSLS libraries.

The following values are valid:

Yes

Specifies that the server labels only volumes that are stored in the library, unless the volume is already labeled or its bar code cannot be read.

If you specify the `LABELSOURCE=PROMPT` option, the volume is moved into the drive from its location in the library or entry and exit ports. The server prompts you to issue the REPLY command that contains the label string, and that label is written to the tape.

Bulk

Specifies that the server searches the library entry/exit ports for usable volumes to label. This option is only valid for SCSI libraries.

If you specify LABELSOURCE=BARCODE, the volume bar code is read. Then, the tape is moved from its location in the library or in the entry/exit ports to a drive where the bar code label is written. After the tape is labeled, it is moved back to its location in the library, to the entry/exit ports, or to a storage slot if the CHECKIN option is specified. For bar code support to work correctly for libraries that are supported by IBM Spectrum Protect, the IBM Spectrum Protect server and the device driver must be at the same level. Bar code support is available for libraries that are supported by IBM Spectrum Protect and that use the IBM Spectrum Protect device driver or the IBM® Magstar® or LTO Ultrium device driver.

Tip: You can use the VOLRANGE or VOLLIST parameter to limit the search.

VOLRange

Specifies a range of volume names that are separated by a comma. Use this parameter to limit the search for volumes to be labeled when you specify SEARCH=YES (349X, ACSLS, and SCSI libraries) or SEARCH=BULK (SCSI libraries only). If there are no volumes in the library that are within the specified range, the command completes without errors.

You can specify only volume names that can be numerically incremented. In addition to the incremental area, a volume name can include an alphanumeric prefix and an alphanumeric suffix, for example:

Parameter	**Description**
`volrange=bar110,bar130`	The 21 volumes are labeled: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	The 3 volumes are labeled: bar11a, bar12a, bar13a.
`volrange=123400,123410`	The 11 volumes are labeled: 123400, 123401, ...123409, 123410.

VOLList

Specifies a list of volumes. Use this parameter to limit the search for volumes to be labeled when you specify SEARCH=YES (349X, ACSLS, and SCSI libraries) or SEARCH=BULK (SCSI libraries only). If there are no volumes in the library that are in the list, the command completes without errors. The VOLLIST parameter can also be the source of names to be used to label volumes if the LABELSOURCE parameter is set to VOLLIST. If LABELSOURCE=VOLLIST, you must specify the VOLLIST parameter.

The following values are valid:

volume_name

Specifies the names of one or more values that are used for the command. For example: `VOLLIST=TAPE01,TAPE02`.

FILE:file_name

Specifies the name of a file that contains a list of volumes for the command. In the file, each volume name must be on a separate line. Blank lines and comment lines that begin with an asterisk are ignored. For example, to use volume TAPE01, TAPE02 and TAPE03, create a file that is named TAPEVOL that contains these lines:

```
TAPE01
TAPE02
TAPE03
```

You can specify the volumes for the command as follows: `VOLLIST=FILE:TAPEVOL`.

Remember: The file name is case-sensitive.

LABELSource
: Specifies how or whether the server reads sequential media labels of volumes. This option is only valid for SCSI libraries. Specify this parameter only when SEARCH=YES or SEARCH=BULK.
You can specify the following values:

  Prompt
  : The server prompts for volume names as necessary.

  Barcode
  : The server attempts to read the bar code label. If the attempt fails, the server does not label the volume and displays a message.
  Important: For bar code support to work properly, the appropriate device drivers must be installed for the libraries.

  Vollist
  : This option applies only to SCSI libraries. The server attempts to read the specified file or list of files. If the attempt fails, the server does not label the volumes and displays a message.

OVERWRITE
: Specifies whether the server attempts to overwrite existing labels. This parameter is optional. The default is NO. You can specify the following values:

  No
  : Specifies that the server labels only unlabeled volumes. For StorageTek VolSafe volumes, the value must be NO.

  Yes
  : Specifies that the server overwrites existing labels only if both the existing label and the prompted or bar code label are not already defined in either the server storage pool or volume history list.

WAITTime
: Specifies the number of minutes that the server waits for you to reply or respond to a request. Specify a value in the range 0-9999. If you want to be prompted by the server, specify a wait time greater than zero. The default value is 60 minutes. For example, suppose that the server prompts you to insert a tape into the entry/exit port of a library. If you specified a wait time of 60 minutes, the server issues a request and wait 60 minutes for you to reply. Alternatively, suppose that you specify a wait time of 0. If you inserted a tape, a wait time of zero causes the operation to continue without prompting. If you did not insert a tape, a wait time of zero causes the operation to fail.

Example: Automatically label library volumes

Label tapes in a SCSI library named `AUTO` automatically as you are checking in the volumes.

```
label libvolume auto checkin=scratch search=yes labelsource=barcode
overwrite=yes
```

Example: Label sequential library volumes

Label 3 volumes from `bar11a` to `bar13a` in a SCSI library named ABC. When you issue the following command, the three volumes are labeled: `bar11a`, `bar12a`, `bar13a`.

```
label libvolume abc checkin=scratch search=yes volrange=bar11a,bar13a
labelsource=barcode
```

Related commands

Table 1. Commands related to LABEL LIBVOLUME

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CANCEL PROCESS	Cancels a background server process.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE LIBRARY	Defines an automated or manual library.

Command	Description
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.
QUERY PROCESS	Displays information about background processes.
REPLY	Allows a request to continue processing.
UPDATE LIBVOLUME	Changes the status of a storage volume.

LOAD DEFALERTTRIGGERS (Load the default set of alert triggers)

Use this command to load the default set of alert triggers to the IBM Spectrum Protect™ server.

For a newly installed server, a default set of messages is defined to trigger alerts. You can modify or delete default alert triggers. Use this command to complete the following tasks:

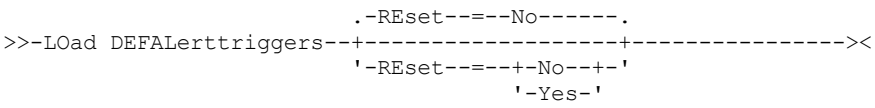
- Load the default set of alert triggers, restoring any that were deleted.
- Replace all alert triggers with the original default set.

By default, this command does not delete other alert triggers that were created, and does not replace default alert triggers that were modified. To delete all alert triggers and restore the original set of default alert triggers, specify RESET=yes.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

REset
: Specifies whether you want to replace all of your alert triggers with the default set of alert triggers. This parameter is optional. The default value is No. Possible values are:

  No
  : Specifies that the default alert triggers are added only. The original default alert triggers are added to the server. Existing triggers are not deleted. If a default trigger exists on the server, it is not replaced or modified.

  Yes
  : Specifies that the alert triggers are restored to the original defaults. All alert triggers are deleted and then the original set of default alert triggers are added.

Example: Load the default alert triggers on the server

Load the default triggers to restore any that were deleted. Issue the command:

```
load defalerttriggers
```

Example: Replace all alert triggers on the server with the default alert triggers

Delete all alert triggers on the server and replace them with the original defaults. Issue the command:

```
load defalerttriggers reset=yes
```

Related commands

Table 1. Commands related to LOAD DEFALERTTRIGGERS

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.

LOCK commands

Use the LOCK command to prevent users from accessing the server.

- LOCK ADMIN (Lock out an administrator)
- LOCK NODE (Lock out a client node)
- LOCK PROFILE (Lock a profile)

LOCK ADMIN (Lock out an administrator)

Use this command to prevent an administrator from accessing the server. The administrator is locked out until a system administrator uses the UNLOCK ADMIN command to reestablish access for the administrator.

You can use the authentication filter to lock all administrators, excluding console administrators. After configuring an LDAP directory server for password authentication, you can lock administrators to force them to create passwords that authenticate with an LDAP server.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-LOCK Admin--+-*----------+--+------------------------------+->< 
               '-admin_name-'  '-AUTHentication--=--+-LOcal-+-'
                                                    '-LDap--'
```

Parameters

admin_name (Required)
: Specifies the name of the administrator to be locked out. You can use wildcard characters to specify the administrator name. You do not have to enter an administrator name if you want to lock all of the administrators according to their authentication method. Use the wildcard with an authentication method to lock multiple administrators.

AUTHentication
: Specifies the method of authentication that the administrator uses to log in.

  LOcal
  : Specifies to lock administrators who authenticate to the IBM Spectrum Protect™ server.

  LDap
  : Specifies to lock administrators who authenticate to the LDAP directory server.

Example: Lock out an administrator

Lock out the administrator CLAUDIA. Issue the command:

```
lock admin claudia
```

Example: Lock out all administrators who authenticate to the IBM Spectrum Protect server database

Use the wildcard character (*) to lock all the administrators who authenticate their passwords locally. Console administrators are not affected by this command. Issue the following command:

```
lock admin * authentication=local
```

Related commands

Table 1. Commands related to LOCK ADMIN

Command	Description
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
UNLOCK ADMIN	Enables a locked administrator to access IBM Spectrum Protect.

LOCK NODE (Lock out a client node)

Use this command to prevent a client node from accessing the server. A locked client node cannot perform any IBM Spectrum Protect™ operations, even if the operations are scheduled.

After configuring an LDAP directory server for password authentication, you can lock nodes to force them to use passwords that authenticate with an LDAP server.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node belongs.

Syntax

```
>>-LOCK Node--+-*---------+--+------------------------------+--><
              '-node_name-'  '-AUTHentication--=--+-LOcal-+-'
                                                  '-LDap--'
```

Parameters

node_name
: Specifies the name of the client node to lock out. You can use a wildcard character instead of a node name if you want to lock all of the nodes according to their method of authentication.

AUTHentication
: Specifies the method of password authentication that is needed to log into a node.

  LOcal
  : Specifies to lock nodes that authenticate with the IBM Spectrum Protect server.

  LDap
  : Specifies to lock nodes that authenticate with an LDAP directory server.

Example: Lock a specific client node

Lock the client node SMITH.

```
lock node smith
```

Example: Lock all nodes that authenticate to the local IBM Spectrum Protect database

Issue the following command to lock all nodes that authenticate with the IBM Spectrum Protect server:

```
lock node * authentication=local
```

Related commands

Table 1. Commands related to LOCK NODE

Command	Description
QUERY NODE	Displays partial or complete information about one or more clients.
UNLOCK NODE	Enables a locked user in a specific policy domain to access the server.

LOCK PROFILE (Lock a profile)

Use this command on a configuration manager to temporarily lock a profile so that configuration information is not distributed to subscribing managed servers.

You can use this command when you are making multiple updates to your configuration and do not want to distribute this information until the changes are completed.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                                .-60------.
>>-LOCK PROFIle--profile_name--+---------+---------------------><
                                '-minutes-'
```

Parameters

profile_name (Required)
: Specifies the profile to lock. You can use wildcard characters to indicate multiple names.

minutes
: Specifies the time, in minutes, before IBM Spectrum Protect™ unlocks the configuration profile. Specify an integer from 0 to 10000. The default is 60 minutes. If you specify 0, the configuration profile will not unlock automatically. Use the UNLOCK PROFILE command to unlock the profile before the time period elapses, or to unlock it if you have specified a value of 0. This parameter is optional.

Example: Lock a profile for a specific amount of time

Lock a profile named DELTA for 30 minutes.

```
lock profile delta 30
```

Related commands

Table 1. Commands related to LOCK PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.

Command	Description
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

MACRO (Invoke a macro)

Use this command to invoke a file from the administrative command line that contains one or more IBM Spectrum Protect™ administrative commands to be performed.

Restriction: Use this command with administrative command-line clients only.

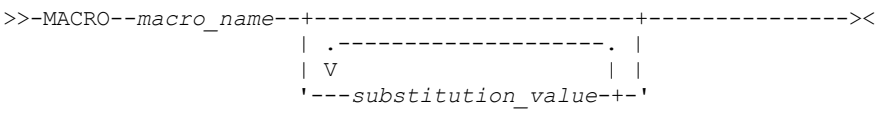
A macro is a file that contains one or more IBM Spectrum Protect administrative commands. You can only issue a macro from the administrative client in batch or interactive mode. A macro is stored as a file on the administrative client machine (or system). Macros are not distributed across servers and cannot be scheduled on the server.

Creating a macro to enter commands can be helpful when you want to issue commands that are used repeatedly, to issue commands that contain several parameters, or to process related commands in a specific order. After you create a macro, you can update the information it contains and use it again, or you can copy the macro file, make changes to the copy, and then run the copy.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

macro_name (Required)
: Specifies the name of the macro.

substitution_value
: Specifies the value for a substitution variable in a macro. When you use a substitution variable, you can reuse a macro whenever you need to perform the same task for different objects or with different parameter values. To specify a value that contains blanks, you must enclose the value in quotation marks. This parameter is optional.

Example: Create a macro to register a new administrator

Create a macro file named REGNG. Use the macro to register and grant authority to a new administrator. Write the macro as follows:

```
/* Register and grant authority to a new administrator */
REGister Admin jones passwd        -
CONtactinfo="x1235"
GRant AUTHority jones              -
CLasses=Policy
```

Issue the following command to run the macro:

```
macro regng.mac
```

Example: Write a macro using substitution variables

Create a macro file named AUTHRG, containing substitution variables, to register and grant authority to a new administrator. Write the macro as follows:

```
/*   Register and grant authority to a new administrator */
REGister Admin %1 %2  -        /*  Enter userid and password  */
CONtact=%3         /* Enter contact info (in quotes if nec.) */
GRant AUTHority %1  -        /*  Server uses variable already */
-                                      /*  defined by you */
CLasses=%4                     /*  Enter the privilege class  */
```

Issue a command similar to the following, entering the values you want to pass to the server to process the command when you run the macro.

```
macro authrg.mac jones passwd x1235 Policy
```

Related commands

Table 1. Commands related to MACRO

Command	Description
COMMIT	Makes changes to the database permanent.
ROLLBACK	Discards any uncommitted changes to the database since the last COMMIT was executed.

Related concepts:
Administrative client macros

MIGRATE STGPOOL (Migrate storage pool to next storage pool)

Use this command to migrate files from one storage pool to the next storage pool in the storage hierarchy.

This command can only be used with primary storage pools. The storage pool data format cannot be NETAPPDUMP, CELERRADUMP, or NDMPDUMP. Data cannot be migrated into or out of storage pools that are defined with a CENTERA device class.

Only one migration or reclamation process for a given storage pool is allowed at any given time. If a migration or reclamation process is already running for the storage pool, you cannot start another migration process for the storage pool.

You should only use this command if you are not going to use automatic migration for the storage pool. To prevent automatic migration from running, set the HIGHMIG attribute of the storage pool definition to 100.

If you use this command to start a migration process, but the storage pool does not have a next storage pool identified in the hierarchy, a reclamation process is triggered for the source storage pool. To prevent the reclamation process, define the next storage pool in the hierarchy. Then, start the migration process.

The MIGRATE STGPOOL command honors the values of the following parameters on the DEFINE STGPOOL and UPDATE STGPOOL commands:

- MIGPROCESS
- MIGDELAY
- MIGCONTINUE
- NEXTPOOL
- LOWMIG
  Tip: You can override the value of the LOWMIG parameter on DEFINE STGPOOL and UPDATE STGPOOL by specifying a value for the LOWMIG parameter on the MIGRATE STGPOOL command.

The MIGRATE STGPOOL command ignores the value of the HIGHMIG parameter of the storage pool definition. Migration occurs regardless of the value of the HIGHMIG parameter.

This command creates one or more migration processes that can be canceled with the CANCEL PROCESS command. The number of processes is limited by the MIGPROCESS attribute of the storage pool definition. To display information about background

processes, use the QUERY PROCESS command.

Remember: Migrating data from a primary storage pool that is set up for data deduplication to another primary storage pool that is also set up for data deduplication removes duplicate data.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for both the storage pool from which the files are to be migrated and the next storage pool to which files are to be migrated.

Syntax

```
>>-MIGrate STGpool--pool_name--+-------------------+------------>
                               '-LOwmig--=--number-'

                             .-REClaim--=--No------.
>--+----------------------+--+---------------------+------------>
   '-DUration--=--minutes-'  '-REClaim--=--+-No--+-'
                                           '-Yes-'

   .-Wait--=--No------.
>--+------------------+-----------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameters

pool_name (Required)
: Specifies the primary storage pool from which files are to be migrated.

DUration
: Specifies the maximum number of minutes the migration runs before being automatically canceled. When the specified number of minutes elapses, the server will automatically cancel all migration processes for this storage pool. As soon as the processes recognize the automatic cancellation, they end. As a result, the migration might run longer than the value you specified for this parameter. You can specify a number from 1 to 9999. This parameter is optional. If not specified, the server will stop only after the low migration threshold is reached.

LOwmig
: For random-access and sequential-access disk storage pools, specifies that migration should stop when the amount of data in the pool is at or below this percentage of the pool's estimated capacity. This parameter is optional.
  The calculation for sequential-access disk storage pools includes the capacity of all the scratch volumes that are specified for the pool. Because migration is by node or filespace, depending upon collocation, the occupancy of the storage pool can fall below the value that you specified for this parameter. To empty the storage pool, set LOWMIG=0. For other types of sequential-access storage pools, the server stops migration when the ratio of volumes containing data to the total number of volumes in the storage pool is at or below this percentage. The total number of volumes includes the maximum number of scratch volumes. You can specify a number from 0 to 99 for this optional parameter. The default value is the LOWMIG attribute of the storage pool definition.

RECLaim
: Specifies whether reclamation is attempted for the storage pool before completing the migration. This parameter can only be specified for a sequential-access storage pool. This parameter is optional. The default is No. Possible values are:

  No
  : Specifies that the server will not attempt a reclamation before starting the migration.

  Yes
  : Specifies that the server will attempt reclamation before starting the migration. Any volumes in the storage pool that meet the reclamation threshold as specified by the RECLAIM attribute of the storage pool definition will be reclaimed before completing the migration. If no volumes meet the reclamation threshold or if, after reclamation, the LOWMIG threshold has not been reached, the server will begin the migration. Before reclaiming space for storage pools defined with RECLAMATIONTYPE=SNAPLOCK, the server deletes all empty WORM FILE volumes during reclamation processing that have exceeded their reclaim period.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. This default is No. Possible values are:

No

Specifies that the server processes this command in the background.

You can continue with other tasks while the command is being processed. Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files may have already been migrated before the cancellation.

Yes

Specifies that the server processes this command in the foreground. The operation must complete before you can continue with other tasks. The server then displays the output messages to the administrative client when the operation completes. Messages are also displayed either in the activity log or the server console, or both, depending on where the messages are logged.
Note: You cannot specify WAIT=YES from the server console.

Example: Migrate a storage pool to the next storage pool

Migrate data from the storage pool named BACKUPPOOL to the next storage pool. Specify that the server should end the migration as soon as possible after 90 minutes.

```
migrate stgpool backuppool duration=90
```

Related commands

Table 1. Commands related to MIGRATE STGPOOL

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY PROCESS	Displays information about background process.
QUERY STGPOOL	Displays information about storage pools.
RECLAIM STGPOOL	Performs reclamation for the storage pool.

Related information:
Migrating files in a storage pool hierarchy

MOVE commands

Use the MOVE commands to either transfer backup or archive data between storage pools, or to move disaster recovery media on and off site.

- MOVE CONTAINER (Move a container)
- MOVE DATA (Move files on a storage pool volume)
- MOVE DRMEDIA (Move disaster recovery media offsite and back onsite)
- MOVE GRPMEMBER (Move a server group member)
- MOVE MEDIA (Move sequential-access storage pool media)
- MOVE NODEDATA (Move data by node in a sequential access storage pool)

AIX | Linux | Windows

MOVE CONTAINER (Move a container)

Use this command to move the contents of a storage pool container to another container if a storage pool directory is removed or if a container is damaged. You can also use the command to consolidate data and reclaim space. You can issue this command for directory containers and cloud containers.

If the data in a storage pool is fragmented, the command consolidates the data:

- For a directory-container storage pool, the command potentially reduces the number of containers.
- For a cloud-container storage pool, the command consolidates the data into a smaller container.

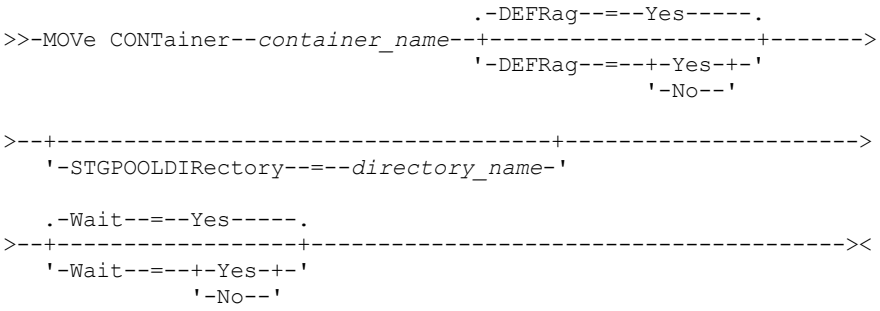
In addition, for directory-container storage pools, you can use this command to move the contents of a storage pool container under these conditions:

- When you upgrade hardware
- If I/O errors occur on a disk

Privilege class

To issue this command, you must have restricted storage privilege.

Syntax



Parameters

container_name (Required)
: Specifies the name of the container to move. You must specify the full path name of the container.

DEFRag
: Specifies whether the contents of the container are consolidated into existing containers during a MOVE CONTAINER operation. This parameter is optional.

  The following values are possible:

  Yes
  : This is the default value. The container contents are moved in the following way:

    - For a container in a directory-container storage pool, the contents are moved into one or more existing containers. If the existing containers have insufficient space, a container is created and any remaining data is allocated to the new container.
    - For a container in a cloud-container storage pool, the contents are moved into a single new cloud container.

  No
  : The contents are moved into a newly created container.
    Restriction: If you are issuing the MOVE CONTAINER command for a cloud container, you cannot specify DEFRAG=NO.

    In some cases, especially if you encrypt data, you might have to create additional containers and allocate the data to the new containers to ensure sufficient space. For instructions, see technote 7050411.

STGPOOLDIRectory
: Specifies the name of the storage pool directory to which the container is moved. This parameter is optional.

  If you specify a storage pool directory, it must be in the same storage pool as the original container. The storage pool directory is used for the new container. If you don't specify a storage pool directory, the IBM Spectrum Protect™ server selects a storage pool directory from the same storage pool.

  Restriction: If you are issuing the MOVE CONTAINER command for a cloud container, do not specify the STGPOOLDIRECTORY parameter.

Wait
: Specifies whether to wait for the IBM Spectrum Protect server to process this command in the foreground. This parameter is optional. You can specify one of the following values:

No

The server processes this command in the background and you can continue with other tasks while the command is processing. Messages that are related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged. This is the default.

Yes

The server processes this command in the foreground. The operation must complete processing before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.
Restriction: You cannot specify the WAIT=YES parameter from the server console.

Example: Move a container in a directory-container storage pool

AIX Linux Move a container, 0000000000000001.dcf, from the /data1/storage/dir1 storage pool directory to the /data/storage/dir2 storage pool directory.

```
move container /data1/storage/dir1/00/0000000000000001.dcf
stgpooldir=/data/storage/dir2
```

Windows Move a container, 0000000000000001.dcf, from the e:\data1\storage\dir1 storage pool directory to the e:\data\storage\dir2 storage pool directory.

```
move container e:\data1\storage\dir1\00\0000000000000001.dcf
stgpooldir=e:\data\storage\dir2
```

Table 1. Commands related to MOVE CONTAINER

Command	Description
AUDIT CONTAINER commands	Audit directory-container or cloud-container storage pools.
QUERY CONTAINER	Displays information about a container.

MOVE DATA (Move files on a storage pool volume)

Use this command to move files from one storage pool volume to other storage pool volumes.

Restriction: You cannot use this command for volumes that are assigned to copy-container storage pools.
You can move files from a primary storage pool volume only to volumes in the same or a different primary storage pool. You can move files from a copy storage pool volume only to volumes in the same copy storage pool. You can move files from an active-data pool volume only to volumes in the same active-data pool.

In addition to moving data from volumes in storage pools that have NATIVE or NONBLOCK data formats, you can use this command to move data from volumes in storage pools that have NDMP data formats (NETAPPDUMP, CELERRADUMP, or NDMPDUMP). The target storage pool must have the same data format as the source storage pool. If you are moving data out of a storage pool for the purpose of upgrading to new tape technology, the target primary storage pool must be associated with a library that has the new device for the tape drives. IBM Spectrum Protect™ supports backend data movement for NDMP images.

You cannot move data into or out of a storage pool that is defined with a CENTERA device class.

If you are moving files to volumes in the same storage pool, sufficient space must be available on the volumes. Otherwise, the operation fails.

When you move files from a sequential access volume, multiple sequential access volume mounts are required to move files that span volumes.

When you move files from a random access volume, the server erases any cached copies of files on the volume.

After a move data operation completes, a volume might not be empty if one or more files cannot be relocated to another volume because of input/output errors on the device or because errors were found in the file. If needed, you can delete the volume using the option to discard any data. The files with I/O or other errors are then deleted.

You can use this command to move files from an offsite volume in a copy storage pool or active-data pool. Because the offsite volume cannot be mounted, the server obtains the files that are on the offsite volume from either a primary storage pool or another copy storage pool. These files are then written to the destination volumes in the original copy storage pool or active-data pool.

During the data movement process, active-data pools cannot be used to obtain data.

If you run the MOVE DATA command on an offsite volume that contains collocated data, it might be necessary to issue the MOVE DATA command multiple times to move all of the data out of the volume. For example, if you are using filespace collocation groups with an offsite volume that contains filespaces in a collocation group and filespaces that are not in the group, you must issue two MOVE DATA commands. Each MOVE DATA command moves the data for a single collocated or non-collocated group of files.

Do not use the MOVE DATA command if a restore process (RESTORE STGPOOL or RESTORE VOLUME) is running. The MOVE DATA command might cause the restore to be incomplete. If you issue the MOVE DATA command during a restore operation and you receive an error message indicating that one or more files are locked and cannot be moved, you must reissue the MOVE DATA command after the restore operation completes in order to move any remaining files.

Remember:
Issuing this command removes duplicate data when:

- Moving data from a primary storage pool that is set up for data deduplication to another primary storage pool that is also set up for data deduplication.
- Moving data within a copy storage pool that is set up for data deduplication.
- Moving data within an active-data pool that is set up for data deduplication.

A volume in a deduplicated storage pool might contain files that are logically deleted but are still linked by files on other volumes. If you use the MOVE DATA command to move the contents of a deduplicated storage pool volume to a non-deduplicated storage pool, the logically deleted files are not written to the new volume since they do not exist logically. The deleted files are kept on the original volumes for other files to reference. The MOVE DATA process ends successfully but none of the deleted files are moved to the new target volume and the source volume is not deleted. You can issue the QUERY CONTENT command with the FOLLOWLINKS=YES or FOLLOWLINKS=JUSTLINKS parameter to verify whether the volume contains files that are linked by files on other volumes.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to which the volume belongs and also for the new storage pool, if one is specified.

Syntax

```
>>-MOVe Data--volume_name--+-----------------------+------------>
                           '-STGpool--=--pool_name-'

   .-SHREDTONOshred--=--No------.
>--+----------------------------+------------------------------>
   '-SHREDTONOshred--=--+-No--+-'
                        '-Yes-'

                               (1) (2)
   .-RECONStruct--=--No or Yes---------.
>--+-----------------------------------+------------------------>
   '-RECONStruct--=--+-No--+-----------'
                     '-Yes-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Notes:

1. The default is NO if either the source or target storage pool is random access. The default is YES if both the source and target storage pools are sequential access.
2. This parameter is not available or is ignored if the data format is NETAPPDUMP, CELERRADUMP, or NDMPDUMP data.

Parameters

volume_name (Required)
: Specifies the storage pool volume from which to move files.

STGpool

Specifies the primary storage pool to which you want to move files (the target storage pool). This parameter is optional and applies only to moving data from primary storage pool volumes. If you do not specify a value for this parameter, files are moved to other volumes within the same storage pool.

SHREDTONOshred

Specifies whether data is moved from a storage pool that enforces shredding to a storage pool that does not enforce shredding. This parameter is optional. The default value is NO. Possible values are:

No

Specifies that the server will not allow data to be moved from a storage pool that enforces shredding to a storage pool that does not enforce shredding. If the source storage pool enforces shredding and the target storage pool does not, the operation fails.

Yes

Specifies that the server allows data to be moved from a storage pool that enforces shredding to a storage pool that does not enforce shredding. The source data is shredded when the operation is complete. The target data will not be shredded when it is deleted.

RECONStruct

Specifies whether to reconstruct file aggregates during data movement. Reconstruction removes empty space that has accumulated during deletion of logical files from an aggregate. This parameter is optional. If both the source and target storage pools are sequential access, the default value is YES. If either the source or target storage pool is random access, the default is NO.

The parameter is not available or is ignored if any of the following conditions are true:

- The data format is NETAPPDUMP, CELERRADUMP, or NDMPDUMP.
- The data is in a storage pool that is configured for data deduplication.
- The target storage pool for the data movement is configured for data deduplication.

Attention: Reconstruction removes inactive backup files in active-data pools. If you specify RECONSTRUCT=NO when moving the data in an active-data pool that is not configured for data deduplication, inactive backup files remain in the storage pool.

Possible values are:

No

Specifies that reconstruction of file aggregates is not completed during data movement.

Yes

Specifies that reconstruction of file aggregates is completed during data movement. You can only specify this option when both the source and the target storage pools are sequential-access.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is No. Possible values are:

No

Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

The server displays messages that are created from the background process either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If a MOVE DATA background process is canceled, some files may have already moved before the cancellation.

Yes

Specifies that the server processes this command in the foreground. You wait for the command to complete before continuing with other tasks. The server then displays the output messages to the administrative client when the command completes.

Restriction: You cannot specify WAIT=YES from the server console.

Example: Move files on a storage pool volume

Move files from storage pool volume STGVOL.1 to any available volumes assigned to the 8MMPOOL storage pool.

```
move data stgvol.1 stgpool=8mmpool
```

Related commands

Table 1. Commands related to MOVE DATA

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE VOLUME	Deletes a volume from a storage pool.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY PROCESS	Displays information about background processes.
QUERY SHREDSTATUS	Displays information about data waiting to be shredded.
SHRED DATA	Manually starts the process of shredding deleted data.

MOVE DRMEDIA (Move disaster recovery media offsite and back onsite)

Use this command to track volumes that are to be moved offsite and to identify the expired or empty volumes that are to be moved onsite. You can track database backup volumes, and volumes in copy storage pools, container-copy storage pools, and active-data storage pools.

The processing of volumes by this command depends on what the volumes are used for:

Backups of the server database
: To control whether the command processes database backup volumes, use the SOURCE parameter on this command. The command can process volumes that are used for full plus incremental or snapshot database backups. You cannot specify virtual volumes (backup objects that are stored on another server). You can change volumes through each state, or you can use the TOSTATE parameter and skip states to simplify the movements.

Copy storage pools
: The MOVE DRMEDIA command always processes copy storage-pool volumes.

Container-copy storage pools
: By default, volumes in container-copy storage pools are not eligible for processing by the MOVE DRMEDIA command. To process container-copy storage pool volumes, you must issue the SET DRMCOPYCONTAINERSTGPOOL command first, or specify the COPYCONTAINERSTGPOOL parameter on the MOVE DRMEDIA command.

Active-data storage pools
: By default, volumes in active-data storage pools are not eligible for processing by the MOVE DRMEDIA command. To process active-data pool volumes, you must issue the SET DRMACTIVEDATASTGPOOL command first, or specify the ACTIVEDATASTGPOOL parameter on the MOVE DRMEDIA command.

You can use the QUERY ACTLOG command to see whether the MOVE DRMEDIA command was successful. You can also view this information from the server console.

Restriction: Do not run the MOVE DRMEDIA and BACKUP STGPOOL commands concurrently. Ensure that the storage pool backup processes are complete before you issue the MOVE DRMEDIA command.

Privilege class

To issue this command, you must have one of the following privilege classes:

- If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO: operator, unrestricted storage, or system privilege.
- If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES (the default): system privilege.

Syntax

Parameters

volume_name (Required)

Specifies the name of the volume to be processed. You can use wildcard characters. If you use wildcard characters to specify this name, you must also specify the WHERESTATE parameter. The server looks for matching names among the following eligible volumes:

- Database backup volumes, as specified by the SOURCE parameter of this command.
- Copy storage pool volumes from the storage pools named in the COPYSTGPOOL parameter. If you do not use the COPYSTGPOOL parameter, the server processes volumes from copy storage pools that were previously specified in

the SET DRMCOPYSTGPOOL command.
- Container-copy storage pool volumes from the storage pools named in the COPYCONTAINERSTGPOOL parameter. If you do not use the COPYCONTAINERSTGPOOL parameter, the server processes volumes from container-copy storage pools that were previously specified in the SET DRMCOPYCONTAINERSTGPOOL command.
- Active-data storage pool volumes from the storage pools named in the ACTIVEDATASTGPOOL parameter. If you do not use the ACTIVEDATASTGPOOL parameter, the server processes volumes from active-data storage pools that were previously specified in the SET DRMACTIVEDATASTGPOOL command.

Other parameters can also limit the results of the command.

WHERESTate

Specifies the state of volumes to be processed. This parameter is required if the TOSTATE parameter is not specified or if you use a wildcard character in the volume name. For more information, see Table 2 and Table 3. Specify one of the following values:

MOuntable

These volumes contain valid data and are available for onsite processing. The values change to NOTMOUNTABLE if the TOSTATE parameter is not specified.

Depending on the outcome of the REMOVE parameter, the server might eject volumes in an automated library before you change the destination state.

For external libraries, the server sends requests to the external library manager to eject the volumes. It depends on the external library manager whether the volumes are ejected from the library.

NOTMOuntable

These volumes are onsite, contain valid data, and are not available for onsite processing. The values change to COURIER if the TOSTATE parameter is not specified.

COUrier

These volumes are with the courier and being moved offsite. The values change only to VAULT.

VAULTRetrieve

These volumes are at the offsite vault and do not contain valid data. The values change to COURIERRETRIEVE if the TOSTATE parameter is not specified.

COURIERRetrieve

These volumes are with the courier and being moved onsite. The values change only to ONSITERETRIEVE. The server deletes the volume records of the database backup and scratch copy storage pool volumes from the database.

BEGINDate

Specifies the beginning date that is used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command changes the volume to its current state on or after the specified date. The default is the earliest date for which volume information exists.

You can specify the date by using one of the following values:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date.	`09/15/1998`
TODAY	The current date.	`TODAY`
TODAY-days or -days	The current date minus days specified.	`TODAY-7` or `-7` To identify volumes that were changed to their current state a week ago, you can specify `TODAY-7` or `-7`.
EOLM (end of last month)	The last day of the previous month.	`EOLM`
EOLM-days	The last day of the previous month minus days specified.	`EOLM-1` To include files that were active a day before the last day of the previous month.
BOTM (beginning of this month)	The first day of the current month.	`BOTM`

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	`BOTM+9` To include files that were active on the 10th day of the current month.

ENDDate

Specifies the ending date that is used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command changes the volume to its current state on or before the specified date. The default is the current date.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date.	`09/15/1998`
TODAY	The current date.	`TODAY` To identify volumes that were changed to their current state today, specify `TODAY`.
TODAY-days or -days	The current date minus days specified. The maximum number of days is 9999.	`TODAY-1` or `-1` To identify volumes that were changed to their current state a week ago, you can specify `TODAY-1` or `-1`.
EOLM (end of last month)	The last day of the previous month.	`EOLM`
EOLM-days	The last day of the previous month minus days specified.	`EOLM-1` To include files that were active a day before the last day of the previous month.
BOTM (beginning of this month)	The first day of the current month.	`BOTM`
BOTM+days	The first day of the current month, plus days specified.	`BOTM+9` To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time that is used to select volumes for processing. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command changes the volume to its current state on or after the specified time and date. The default is midnight (00:00:00) on the date that is specified with the BEGINDATE parameter.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date.	`12:33:28`
NOW	The current time on the specified begin date.	`NOW`
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified begin date.	`NOW+03:00` or `+03:00`
NOW-HH:MM or -HH:MM	The current time minus hours and minutes on the specified begin date.	`NOW-03:30` or `-03:30` If you issue the MOVE DRMEDIA command at 9:00 with BEGINTIME=NOW-03:30 or BEGINTIME=-03:30, the server identifies the volumes that were changed to their current state at 5:30 on the begin date that you specify.

ENDTime

Specifies the ending time that is used to select volumes for processing. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command changes the volume to its current state on or after the specified time and date. The default is 23:59:59.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date.	`12:33:28`
NOW	The current time on the specified end date.	`NOW`
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified end date.	`NOW+03:00` or `+03:00` If you issue the MOVE DRMEDIA command at 9:00 with ENDTIME=NOW+03:30 or ENDTIME=+03:30, the server identifies the volumes that were changed to their current state at 12:30 on the end date you specify.
NOW-HH:MM or -HH:MM	The current time minus hours and minutes on the specified end date.	`NOW-03:30` or `-03:30`

COPYCONtainerstgpool
Specifies the name of the container-copy storage pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. If you use wildcard characters to specify this name, you must also specify the WHERESTATE parameter.

The container-copy storage pools that are specified with this parameter override storage pools that are specified with the SET DRMCOPYCONTAINERSTGPOOL command. If this parameter is not specified, the server selects the storage pools as follows:

- If the SET DRMCOPYCONTAINERSTGPOOL command was previously issued with valid container-copy storage pool names, the server processes only those storage pools.
- If the SET DRMCOPYCONTAINERSTGPOOL command was not issued, or if all of the container-copy storage pools were removed by using the SET DRMCOPYCONTAINERSTGPOOL command, the server processes all container-copy storage pool volumes based on the setting of the WHERESTATE parameter. If the parameter is set to a value of NOTMOUNTABLE, COURIER, VAULTRETRIEVE, or COURIERRETRIEVE, the volumes are processed. If the value is MOUNTABLE, the volumes are not processed.

COPYstgpool
Specifies the name of the copy storage pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. If you use wildcard characters to specify this name, you must also specify the WHERESTATE parameter.

The copy storage pools that are specified with this parameter override copy storage pools that are specified with the SET DRMCOPYSTGPOOL command. If this parameter is not specified, the server selects the storage pools as follows:

- If the SET DRMCOPYSTGPOOL command was previously issued with valid copy storage pool names, the server processes only those storage pools.
- If the SET DRMCOPYSTGPOOL command was not issued, or if all of the copy storage pools are removed by using the SET DRMCOPYSTGPOOL command, the server processes all copy storage pool volumes in the specified state. The states available are MOUNTABLE, NOTMOUNTABLE, COURIER, VAULTRETRIEVE, or COURIERRETRIEVE.

ACTIVEDatastgpool
Specifies the name of the active-data pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. If you use wildcard characters to specify this name, you must also specify the WHERESTATE parameter.

The active-data pools that are specified with this parameter override active-data pools that are specified with the SET DRMACTIVEDATASTGPOOL command. If this parameter is not specified, the server selects the storage pools in the following way:

- If the SET DRMACTIVEDATASTGPOOL command was previously issued with valid active-data pool names, the server processes only those storage pools.
- If the SET DRMACTIVEDATASTGPOOL command was not issued, or all of the active-data pools are removed by using the SET DRMACTIVEDATASTGPOOL command, the server processes all active-data pool volumes in the specified state. The states available are NOTMOUNTABLE, COURIER, VAULTRETRIEVE, or COURIERRETRIEVE. Volumes in the MOUNTABLE state are not processed.

Source
Specifies whether to include database backup volumes for processing. This parameter is optional. The default is DBBACKUP. Specify one of the following values:

DBBackup
: Specifies that the server includes full and incremental database backup volumes for processing.

DBSnapshot
: Specifies that the server includes database snapshot backup volumes for processing.

DBNOne
: Specifies that the server does not include any database backup volumes for processing.

REMove
: Specifies that the server tries to move the volume out of the library and into the convenience I/O station or entry/exit ports. This parameter is optional. Possible values are YES, NO, BULK, and UNTILEEFULL. The default is BULK. The response of the server to each value and the default value depends on the type of library.
Restriction: You can use the REMOVE=UNTILEEFULL option only with the library type SCSI.

SCSI libraries
: The response of the server to the command depends on whether the library has entry/exit ports, and if so, whether a port is available for use. See the following table.

Table 1. Server response for SCSI libraries

Library characteristic	**Server response when you specify REMOVE=YES**	**Server response when you specify REMOVE=BULK**	**Server response when you specify REMOVE=NO**	**Server response when you specify REMOVE=UNTILEEFULL**
Library has no entry/exit ports	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.
Library has entry/exit ports and an entry/exit port is available	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.	The server specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.

Library characteristic	Server response when you specify REMOVE=YES	Server response when you specify REMOVE=BULK	Server response when you specify REMOVE=NO	Server response when you specify REMOVE=UNTILEFULL
Library has entry/exit ports, but no ports are available	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and to issue a REPLY command.	The server waits for a port to be made available.	The server specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.	The command fails and any remaining eligible volumes are not processed. Make the port available and issue the command again.

349X libraries

REMOVE=YES
: The 3494 Library Manager ejects the cartridge to the convenience I/O station.

REMOVE=BULK
: The 3494 Library Manager ejects the cartridge to the high-capacity output facility.

REMOVE=NO
: The 3494 Library Manager does not eject the volume. The server leaves the cartridge in the library in the INSERT category for use by other applications.

ACSLS libraries

REMOVE=YES or REMOVE=BULK
: The server ejects the cartridge to the convenience I/O station.

  The server then deletes the volume entry from the server library inventory.

  When you move volumes from the MOUNTABLE state with REMOVE=YES specified, the MOVE MEDIA command uses more than one slot in the CAP for a StorageTek library with ACSLS.

REMOVE=NO
: The server does not eject the cartridge.

  The server deletes the volume entry from the server library inventory and leaves the volume in the library.

External libraries
: You can specify REMOVE=YES, REMOVE=BULK, or REMOVE=NO. For any value, the server requests the external library manager to eject the volume from the library.

  It depends on the external library manager whether the volume is ejected from the library. Refer to the external library documentation for information about the procedures to follow when you use the MOVE DRMEDIA command to track volumes.

TOSTate
: Specifies the destination state of the volumes that are processed. This parameter is required if the WHERESTATE parameter is not specified. If you specify TOSTATE parameter but not WHERESTATE parameter, you must specify the volume name. Wildcard characters are not allowed. See Table 2 and Table 3.
  Specify one of the following values:

NOTMOuntable
: Specifies that volumes are to change to the NOTMOUNTABLE state. This value is valid only if the volumes are in the MOUNTABLE state.

  If volumes are in an automated library, the server might eject the volumes from the library before you change them to the NOTMOUNTABLE state, depending on the behavior of the REMOVE parameter.

For external libraries, the server sends requests to the external library manager to eject the volumes. Whether the volumes are ejected from the library depends on the external library manager. Refer to the external library documentation for information about the procedures to follow when you use the MOVE DRMEDIA command to track the volumes.

COUrier
: Specifies that volumes are to change to the COURIER state. This value is valid only if the volumes are in the MOUNTABLE or NOTMOUNTABLE state.

  Depending on the behavior of the REMOVE parameter and whether volumes are in an automated library, the server might eject the volumes from the library before you change them to the COURIER state.

  For external libraries, the server sends requests to the external library manager to eject the volumes. Whether the volumes are ejected from the library depends on the external library manager. Refer to the external library documentation for information about the procedures to follow when you use the MOVE DRMEDIA command to track the volumes.

VAult
: Specifies that volumes are to change to the VAULT state. This value is valid only if the volumes are in the MOUNTABLE, NOTMOUNTABLE, or COURIER state.

  Depending on the behavior of the REMOVE parameter and whether volumes are in an automated library, the server might eject the volumes from the library before you change them to the VAULT state.

  For external libraries, the server sends requests to the external library manager to eject the volumes. Whether the volumes are ejected from the library depends on the external library manager. Refer to the external library documentation for information about the procedures to follow when you use the MOVE DRMEDIA command to track the volumes.

COURIERRetrieve
: Specifies that volumes are to change to the COURIERRETRIEVE state. This value is valid only if the volumes are in the VAULTRETRIEVE state.

ONSITERetrieve
: Specifies that volumes are to change to the ONSITERETRIEVE state. This value is valid only if the volumes are in the VAULTRETRIEVE or COURIERRETRIEVE state. For database backup and scratch copy storage pool volumes that are changing to the ONSITERETRIEVE state, the server deletes the volume records from the database.

WHERELOcation
: Specifies the current location of the volumes. This parameter is optional. The maximum length of the location is 255 characters. Enclose the text in quotation marks if it contains any blank characters.

TOLOcation
: Specifies the destination location of the volumes. This parameter is optional. The maximum length of the location that is specified is 255 characters. Enclose the text in quotation marks if it contains any blank characters. If you do not specify the destination location, the location that is defined by the SET DRMNOTMOUNTABLE command is used.

CMd
: Specifies a command to be issued for each volume that is processed by the MOVE DRMEDIA command. DRM writes the commands to a file that is specified by the CMDFILENAME parameter. After the MOVE DRMEDIA operation is completed, the commands in the file can be issued. The command can contain up to 255 characters. If the command contains more than 240 characters, it is split into multiple lines, and continuation characters (+) are added. You might need to alter the continuation character based on the operating system. This parameter is optional.

  command
  : The command string that is enclosed in quotation marks. The string must not include embedded quotation marks. For example, the following CMD parameter is valid:

    ```
    cmd="checkin libvol lib8mm &vol status=scratch"
    ```

    The following example is not a valid way to specify the CMD parameter:

    ```
    cmd=""checkin libvol lib8mm" &vol status=scratch""
    ```

    The command can include substitution variables. The variables are not case-sensitive, and must not contain blank spaces after the ampersand (&). You can specify the following values:

    &VOL
    : A volume name.

&LOC
A volume location.
&VOLDSN
The file name to be written into the sequential access media labels. For example, if the applicable device class sets BKP as the tape volume prefix, a copy storage pool tape volume file name might be BKP.BFS and a database backup tape volume file name might be BKP.DBB.
&NL
The new line character. When you use the new line character, the command is split at the &NL variable. If required, you must specify the appropriate continuation character before the &NL character. If the &NL character is not specified and the command line is greater than 240 characters, the line is split into multiple lines and continuation characters (+) are added.

AIX Linux CMDFilename
AIX Linux Specifies the fully qualified name of the file that contains the commands that are specified by CMD parameter. This parameter is optional.

If you do not specify a file name or if you specify a null string (""), DRM uses the file name that is specified by the SET DRMCMDFILENAME command. If you do not specify a file name with the SET DRMCMDFILENAME command, DRM generates a file name by appending `exec.cmds` to the directory path name of the current working directory of the server.

If the operation fails after the command file is created, the file is not deleted.

Windows CMDFilename
Windows Specifies the fully qualified name of the file that contains the commands that are specified by CMD parameter. This parameter is optional.

The maximum length of the file name is 259 characters. If you do not specify a file name or if you specify a null string (""), DRM uses the file name that is specified by the SET DRMCMDFILENAME command. If you do not specify a file name with the SET DRMCMDFILENAME command, DRM generates a file name by appending `exec.cmd` to the directory that represents this instance of the server (typically the directory from which the server was installed). The DRM allocates the file name that is specified or generated. If the file name exists, DRM tries to use it; any existing data is overwritten. If this happens and the executable commands in the file have not been run, issue QUERY DRMEDIA command to rebuild the executable commands for the desired date and volume transition.

If the MOVE DRMEDIA command fails and none of the command string that is specified with the CMD parameter is written for the volume that successfully moved, the allocated file name is deleted.

APPend
Specifies whether to overwrite any existing contents of the command file or append the commands to the file. This parameter is optional. The default is NO. Specify one of the following values:

No
DRM overwrites the contents of the file.
Yes
DRM appends the commands to the file.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is NO. Specify one of the following values:

No
Specifies that the server processes this command in the background.

Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To see whether the operation was successful, issue the QUERY ACTLOG command.

Yes
Specifies that the server processes this command in the foreground. Wait for the command to complete before you continue with other tasks. The server then displays the output messages to the administrative client.
Restriction: You cannot specify WAIT=YES from the server console.

CAP

Specifies which cartridge access port (CAP) to use for ejecting volumes if you specify REMOVE=YES. This parameter applies to volumes in ACSLS libraries only. If the CAP priority value is set to 0 in the library, this parameter is required. If a CAP priority value greater than 0 is set in the library, this parameter is optional. By default, all CAPs initially have a priority value of 0, which means that ACSLS does not automatically select the CAP.
To display valid CAP identifiers (*x,y,z*), issue the QUERY CAP command with ALL specified from the Automated Cartridge System System Administrator (ACSSA) console on the ACSLS server host. The identifiers are as follows:

x
: The Automated Cartridge System (ACS) ID. This identifier can be a number in the range 0 - 126.

y
: The Library Storage Module (LSM) ID. This identifier can be a number in the range 0 - 23.

z
: The CAP ID. This identifier can be a number in the range 0 - 11.

For more information, see the StorageTek documentation.

Rules for destination states and destination locations

The following table shows how DRM determines the destination state and location of a volume.

Destination state

- The value of the TOSTATE parameter that was specified
- The next state of the WHERESTATE parameter that was specified, if the TOSTATE parameter was not specified

Destination location

- The value of the TOLOCATION parameter that was specified
- The location of the TOSTATE parameter that was specified, if the TOLOCATION parameter was not specified
- The location of the next state of the WHERESTATE parameter that was specified, if the TOLOCATION and TOSTATE parameters are not specified

Table 2. Volume destination and location

Parameters specified	Destination state	Destination location
WHERESTATE	The next state of the WHERESTATE	Location of the next state
WHERESTATE, TOSTATE	TOSTATE	Location of the TOSTATE
WHERESTATE, TOLOCATION	The next state of the WHERESTATE	TOLOCATON
WHERESTATE, TOSTATE, TOLOCATION	TOSTATE	TOLOCATION
TOSTATE	TOSTATE	Location of the TOSTATE
TOSTATE, WHERELOCATION	TOSTATE	Location of the TOSTATE
TOSTATE, WHERELOCATION, TOLOCATION	TOSTATE	TOLOCATION

Rules for state transitions

The following tables show the state transitions that volumes are eligible for, based on their current state.

Table 3. State transitions for volumes

	Destination state		
The current state of the volume	MOUNTABLE	NOTMOUNTABLE	COURIER
MOUNTABLE	N	Y	Y
NOTMOUNTABLE	N	N	Y
COURIER	N	N	N
VAULT	N	N	N
VAULTRETRIEVE	N	N	N

The current state of the volume	Destination state		
	MOUNTABLE	**NOTMOUNTABLE**	**COURIER**
COURIERRETRIEVE	N	N	N
ONSITERETRIEVE	N	N	N

Table 4. State transitions for volumes

The current state of the volume	Destination state	
	VAULT	**VAULTRETRIEVE**
MOUNTABLE	Y	N
NOTMOUNTABLE	Y	N
COURIER	Y	N
VAULT	N	N
VAULTRETRIEVE	N	N
COURIERRETRIEVE	N	N
ONSITERETRIEVE	N	N

Table 5. State transitions for volumes

The current state of the volume	Destination state	
	COURIERRETRIEVE	**ONSITERETRIEVE**
MOUNTABLE	N	N
NOTMOUNTABLE	N	N
COURIER	N	N
VAULT	N	N
VAULTRETRIEVE	Y	Y
COURIERRETRIEVE	N	Y
ONSITERETRIEVE	N	N

Example: Move disaster recovery media from the NOTMOUNTABLE state

Move disaster recovery media that is in the NOTMOUNTABLE state to the COURIER state, and then query the results.

```
move drmedia * wherestate=notmountable
tostate=courier

query actlog search="MOVE DRMEDIA"

 08/11/1999 11:12:24   ANR0984I Process 10 for MOVE DRMEDIA started
                        in the BACKGROUND at 11:12:24.
 08/11/1999 11:12:24   ANR0610I MOVE DRMEDIA started by HSIAO as
                        process 10.
 08/11/1999 11:12:25   ANR6683I MOVE DRMEDIA: Volume TAPE0P was moved
                        from NOTMOUNTABLE state to COURIER.
 08/11/1999 11:12:25   ANR6683I MOVE DRMEDIA: Volume TAPE1P was moved
                        from NOTMOUNTABLE state to COURIER.
 08/11/1999 11:12:25   ANR6683I MOVE DRMEDIA: Volume DBTP02 was moved
                        from NOTMOUNTABLE state to COURIER.
 08/11/1999 11:12:25   ANR6683I MOVE DRMEDIA: Volume DBTP01 was moved
                        from NOTMOUNTABLE state to COURIER.
 08/11/1999 11:12:25   ANR6682I MOVE DRMEDIA command ended: 4 volumes
                        processed.
 08/11/1999 11:12:25   ANR0611I MOVE DRMEDIA started by HSIAO as
                        process 10 has ended.
 08/11/1999 11:12:25   ANR0985I Process 10 for MOVE DRMEDIA running in
                        the BACKGROUND processed 4 items with a
                        completion state of SUCCESS at 11:12:25.
```

Example: Move disaster recovery media from the MOUNTABLE state

Move disaster recovery media from the MOUNTABLE state to the COURIER state. If the media is in an automated library, MOVE DRMEDIA ejects the media before you change the state.

```
move drmedia * wherestate=mountable tostate=courier wait=yes
```

```
ANR0984I Process 12 for MOVE DRMEDIA started
 in the FOREGROUND at 09:57:17.
ANR0609I MOVE DRMEDIA started as process 12.
ANR0610I MOVE DRMEDIA started by HSIAO as
 process 12.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume TAPE01 in library LIB8MM starting.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume TAPE01 in library LIB8MM completed
 successful.
ANR6683I MOVE DRMEDIA: Volume TAPE01 was moved
 from MOUNTABLE state to COURIER.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume TAPE02 in library LIB8MM starting.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume TAPE02 in library LIB8MM completed
 successful.
ANR6683I MOVE DRMEDIA: Volume TAPE02 was moved
 from MOUNTABLE state to COURIER.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume DBTP05 in library LIB8MM starting.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume DBTP05 in library LIB8MM completed
 successful.
ANR6683I MOVE DRMEDIA: Volume DBTP05 was moved
 from MOUNTABLE state to COURIER.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume DBTP04 in library LIB8MM starting.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME for
 volume DBTP04 in library LIB8MM completed
 successful.
ANR6683I MOVE DRMEDIA: Volume DBTP04 was moved
 from MOUNTABLE state to COURIER.
ANR6682I MOVE DRMEDIA command ended: 4 volumes
 processed.
ANR0611I MOVE DRMEDIA started by HSIAO as
 process 12 has ended.
ANR0985I Process 12 for MOVE DRMEDIA running
 in the FOREGROUND processed 4 items with a
 completion state of SUCCESS at 10:12:25.
```

Example: Move disaster recovery media from the VAULTRETRIEVE state

Move disaster recovery media that is in the VAULTRETRIEVE state to the ONSITERETRIEVE state. Generate a CHECKIN LIBVOLUME command for each volume that is successfully processed and store the commands in a file:

AIX | Linux

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=/drm/move/exec.cmds
cmd="checkin libvol lib8mm &vol status=scratch"
```

Windows

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=c:\drm\move\exec.cmd
cmd="checkin libvol lib8mm &vol status=scratch"
```

Query the results:

```
query actlog search="MOVE DRMEDIA"
```

```
08/13/1999 09:12:24  ANR0984I Process 15 for MOVE DRMEDIA started in
                      the BACKGROUND at 09:12:24.
08/13/1999 09:12:24  ANR0610I MOVE DRMEDIA started by HSIAO as
                      process 15.
```

```
08/13/1999 09:12:24  ANR6684I MOVE DRMEDIA: Volume CSTP01 was deleted.
08/13/1999 09:12:24  ANR6684I MOVE DRMEDIA: Volume CSTP02 was deleted.
08/13/1999 09:12:24  ANR6684I MOVE DRMEDIA: Volume DBTP10 was deleted.
08/13/1999 09:12:24  ANR6684I MOVE DRMEDIA: Volume DBTP11 was deleted.
08/13/1999 09:12:27  ANR6682I MOVE DRMEDIA command ended: 4 volumes
                      processed.
08/13/1999 09:12:42  ANR0611I MOVE DRMEDIA started by HSIAO as process
                       15 has ended.
08/13/1997 09:12:42  ANR0985I Process 15 for MOVE DRMEDIA running in
                      the BACKGROUND processed 4 items with a
                      completion state of SUCCESS at 09:12:42.
```

The volume check-in commands were also created in the file that was specified with the CMDFILENAME parameter:

- AIX Linux /drm/move/exec.cmds
- Windows c:\drm\move\exec.cmd

The file contains these lines:

```
checkin libvol lib8mm CSTP01 status=scratch
checkin libvol lib8mm CSTP02 status=scratch
checkin libvol lib8mm DBTP10 status=scratch
checkin libvol lib8mm DBTP11 status=scratch
```

Tip: To process the CHECKIN LIBVOLUME commands, issue the MACRO command with the file name as the macro name.

Related commands

Table 6. Commands related to MOVE DRMEDIA

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
CANCEL PROCESS	Cancels a background server process.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DISMOUNT VOLUME	Dismounts a sequential, removable volume by the volume name.
PREPARE	Creates a recovery plan file.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.
QUERY PROCESS	Displays information about background processes.
SET DRMACTIVEDATASTGPOOL	Specifies that active-data storage pools are managed by DRM.
AIX Linux Windows SET DRMCOPYCONTAINERSTGPOOL	AIX Linux Windows Specifies the container-copy storage pools that are used in DRM commands.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.
SET DRMCOURIERNAME	Specifies the name of the courier for the disaster recovery media.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.
SET DRMVAULTNAME	Specifies the name of the vault where DRM media is stored.
SET DRMCMDFILENAME	Specifies a file name for containing DRM executable commands.
SET DRMFILEPROCESS	Specifies whether the MOVE DRMEDIA or QUERY DRMEDIA command processes files associated with a device type of file.

Command	Description
SET DRMNOTMOUNTABLENAME	Specifies the location name of the DRM media to be sent offsite.

MOVE GRPMEMBER (Move a server group member)

Use this command to move a member from one server group to another server group. The command fails if the member you are moving has the same name as a current member of the group.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-MOVe GRPMEMber--member_name--from_group--to_group----------><
```

Parameters

member_name (Required)
: Specifies the member (a server or a server group) to move.

from_group (Required)
: Specifies the server group with which the member is currently associated.

to_group (Required)
: Specifies the new server group for the member.

Example: Move a server to another server group

Move member PAYSON from REGION1 group to REGION2 group.

```
move grpmember payson region1 region2
```

Related commands

Table 1. Commands related to MOVE GRPMEMBER

Command	Description
DEFINE GRPMEMBER	Defines a server as a member of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE GRPMEMBER	Deletes a server from a server group.
DELETE SERVERGROUP	Deletes a server group.
QUERY SERVER	Displays information about servers.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

MOVE MEDIA (Move sequential-access storage pool media)

Use this command to manage overflow storage pools. The database tracks media that is moved by using this command.

This command applies to sequential-access primary and copy storage pool volumes that are managed by an automated library (including an external library). The library does not have to be full. One or more sequential-access storage pool volumes can be processed at the same time.

Use the DAYS parameter to identify eligible volumes to be moved. Use the OVERFLOW LOCATION parameter to record the storage location for the moved media.

This command generates a background process that you can view by using the QUERY PROCESS command. To cancel, issue the CANCEL PROCESS command.

To determine whether the command was successful, issue the QUERY ACTLOG command or use the server console.

The volumes that are moved by the MOVE DRMEDIA command for offsite recovery are not processed by the MOVE MEDIA command.

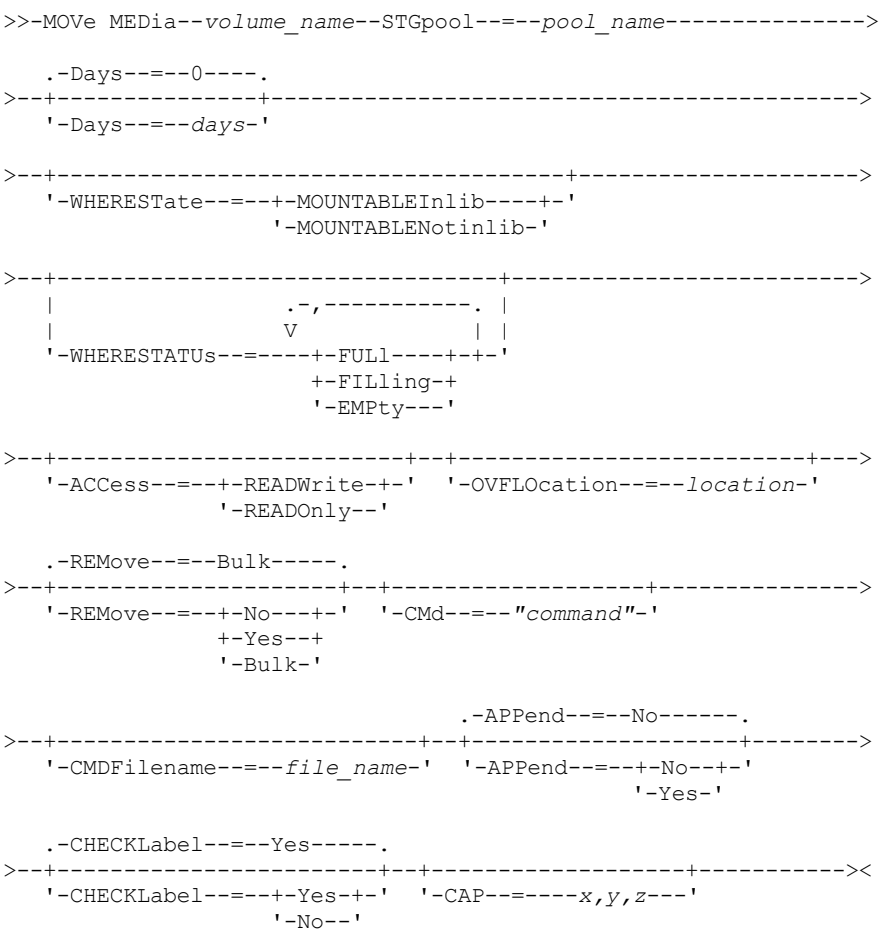
The MOVE MEDIA command does not process copy storage pool volumes with a DRM STATUS value of NOTMOUNTABLE, COURIER, or VAULT.

Privilege class

To issue this command, you must have one of the following privilege classes:

- If the CMD parameter is NOT specified: operator or system privilege.
- If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO: operator, unrestricted storage, or system privilege.
- If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES (the default): system privilege.

Syntax



Parameters

volume_name (Required)
: Specifies the name of the sequential access primary or copy storage pool volume to be processed. You can use a wildcard character to specify the name. All matching volumes are considered for processing.

STGpool (Required)
Specifies the name of the sequential access primary or copy storage pool that is used to select the volumes for processing. You can use a wildcard character to specify the name. All matching storage pools are processed. If the storage pool specified is not managed by an automated library, no volumes are processed.

Days
Specifies the number of days that must elapse after the volume is written or read before the volume is eligible for processing by the command. This parameter is optional. You can specify a number from 0 to 9999. The default value is 0. The most recent of the volumes' last written date or last read date is used to calculate the number of days elapsed.

WHERESTate
Specifies the current state of the volumes to be processed. This parameter is used to restrict processing to the volumes that are in the specified state. This parameter is optional. The default value is MOUNTABLEINLIB.
Possible values are:

MOUNTABLEInlib
Specifies that storage pool volumes are to move from the MOUNTABLEINLIB state to the MOUNTABLENOTINLIB state. Volumes in the MOUNTABLEINLIB state contain valid data and are in the library.

MOUNTABLENotinlib
Specifies that storage pool volumes are to change from the MOUNTABLENOTINLIB state back to the MOUNTABLEINLIB state. Volumes in the MOUNTABLENOTINLIB state might contain valid data and are in the overflow location.

- For empty scratch volumes, the MOVE MEDIA command deletes the volume records so that they can be used again.
- For private volumes, the MOVE MEDIA command resets the volume location to blank, changes the volumes' state to CHECKIN, and changes the last update date to the current date.
- For scratch volumes with data, the MOVE MEDIA command resets the volume location to blank, changes the volumes' state to CHECKIN, and changes the last update date to the current date.

Attention: Volumes in the CHECKIN state might contain valid data and must be checked into the library.

WHERESTATUs
Specifies that the move process must be restricted by volume status. This parameter is optional. You can specify more than one status in a list by separating each status with a comma and no intervening spaces. If you do not specify this parameter, volumes moved from the MOUNTABLEINLIB state to the MOUNTABLENOTINLIB state are restricted to only full volumes, and volumes moved from the MOUNTABLENOTINLIB state to the MOUNTABLEINLIB state are restricted to only empty volumes.

Possible values are:

FULl
Moves volumes with a status of FULL.

FILling
Moves volumes with a status of FILLING.

EMPty
Moves volumes with a status of EMPTY.

ACCess
Specifies how users and system processes access files in the storage pool volume that is moved out from an automated library and stored in an overflow location by the MOVE MEDIA command. This parameter is optional. If you do not specify this parameter, moving volumes from the MOUNTABLEINLIB state to the MOUNTABLENOTINLIB process updates the volumes' access mode to READONLY, and moving volumes from the MOUNTABLENOTINLIB state to the MOUNTABLEINLIB process updates the volumes' access mode to READWRITE.

Possible values are:

READWrite
Specifies that users and system processes can read from and write to files stored on the volume that is in the overflow location. If this value is specified, IBM Spectrum Protect™ requests the volume to be checked into the library when the volume is needed for a read or write operation.

READOnly
Specifies that users and system processes can read but not write to files that are stored on the volume that is in the overflow location. The server requests the volume to be checked into the library only when the volume is needed for a read operation.

OVFLOcation

Specifies the overflow location that is the destination of the volumes that are being processed. The maximum length of the location name is 255 characters. The location name information must be enclosed in quotation marks if it contains any blank characters. If you do not specify an overflow location and the storage pool also has no overflow location identified, the server changes the location of the ejected volume to a null string ("").

REMove

Specifies that the server tries to move the volume out of the library and into the convenience I/O station or entry/exit ports. This parameter is optional. Possible values are YES, BULK, and NO. The default is BULK. The response of the server to each of those options and the default values are described in the following tables.

349X libraries: The following table shows how the server responds for 349X libraries.

Table 1. How the Server Responds for 349X Libraries

REMOVE=YES	**REMOVE=BULK**	**REMOVE=NO**
The 3494 Library Manager ejects the cartridge to the convenience I/O station.	The 3494 Library Manager ejects the cartridge to the high-capacity output facility.	The 3494 Library Manager does not eject the volume. The server leaves the cartridge in the library in the INSERT category for use by other applications.

SCSI libraries: The following table shows how the server responds to YES, BULK, and NO for SCSI libraries.

Table 2. How the Server Responds for SCSI Libraries

If a library...	**And REMOVE=YES...**	**And REMOVE=BULK...**	**And REMOVE=NO**
Does not have entry/exit ports	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and issue a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.
Has entry/exit ports and an entry/exit port is available	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server then prompts you to remove the cartridge from the slot and issue a REPLY command.	The server moves the cartridge to the available entry/exit port and specifies the port address in a message. The server does not prompt you to remove the cartridge and does not request a REPLY command.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.
Has entry/exit ports, but no ports are available	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server then prompts you to remove the cartridge from the slot and issue a REPLY command.	The server waits for an entry/exit port to be made available.	The server leaves the cartridge in its current slot within the library and specifies the slot address in a message. The server does not prompt you to remove the cartridge and does not require a REPLY command.

ACSLS libraries: The following table shows how the server responds for ACSLS libraries.

Table 3. How the Server Responds for ACSLS Libraries

REMOVE=YES or REMOVE=BULK	REMOVE=NO
The server ejects the cartridge to the convenience I/O station. The server then deletes the volume entry from the server library inventory. While moving volumes from the MOUNTABLE state with REMOVE=YES specified, the MOVE MEDIA command uses more than one slot in the CAP for a StorageTek library with ACSLS.	The server does not eject the cartridge. The server deletes the volume entry from the server library inventory and leaves the volume in the library.

External libraries: The following table shows how the server responds for external libraries.

Table 4. How the Server Responds for External Libraries

REMOVE=YES or REMOVE=BULK	REMOVE=NO
The server ejects the cartridge to the convenience I/O station. The server then deletes the volume entry from the server library inventory.	The server does not eject the cartridge. The server deletes the volume entry from the server library inventory and leaves the volume in the library.

CMd

Specifies the creation of executable commands. This parameter is optional. You must enclose your command specification in quotation marks. The maximum length of the command specification is 255 characters. For each volume successfully processed by the MOVE MEDIA command, the server writes the associated commands to a file. Specify the file name with the CMDFILENAME parameter.

AIX Linux If you do not specify the file name, the MOVE MEDIA command generates a default file name by appending the string exec.cmds.media to the IBM Spectrum Protect server directory.

Windows If you do not specify the file name, the MOVE MEDIA command generates a default file name by appending the string exec.cmd.media to the IBM Spectrum Protect server directory.

If the length of the command that is written to the file exceeds 255 characters, it is split into multiple lines and a continuation character, +, is added to all but the last line of the command. You must alter the continuation character according to the requirements of the product that runs the commands.

If you do not specify CMD, the MOVE MEDIA command might not generate any executable commands.

string

Specifies the string to build an executable command. You can specify any free form text for the string. Enclose the full string in quotation marks. For example, the following is a valid executable command specification:

```
CMD="UPDATE VOLUME &VOL"
```

The following is an invalid executable command specification:

```
CMD=""UPDATE VOLUME" &VOL"
```

substitution

Specifies a variable for which you want the command to substitute a value. The possible substitution variables are:

&VOL

Substitute the volume name for &VOL. You can specify lowercase characters, &vol. No spaces or blanks are allowed between ampersand, &, and VOL. If there are spaces or blanks between ampersand and VOL, the MOVE MEDIA command treats them as strings and no substitution is set. If &VOL is not specified, no volume name is set in the executable command.

&LOC

Substitute the volume location for &LOC. You can specify lowercase characters, &loc. No spaces or blanks are allowed between ampersand, &, and LOC. If there are spaces or blanks between ampersand and LOC, the MOVE MEDIA command treats them as strings and no substitution is set. If &LOC is not specified, no location name is set in the executable command.

&VOLDSN

Substitute the volume file name for &VOLDSN. An example of a storage pool tape volume file name that uses the default prefix ADSM is ADSM.BFS. If &VOLDSN is not specified, no volume file name is set in the executable command.

&NL

Substitute a new line character for &NL. When &NL is specified, the MOVE MEDIA command splits the command at the position where the &NL is and does not append any continuation character. The user is responsible for specifying the correct continuation character before the &NL if one is required. The user is also responsible for the length of the line written. If the &NL is not specified and the length of the command line exceeds 255, the command line is split into multiple lines and a continuation character, +, is added to all but the last line of the command.

CMDFilename
Specifies the full path name of a file that contains the commands that are specified with CMD. This parameter is optional. The maximum length of the file name is 1279 characters.

AIX Linux If you do not specify a file name, the MOVE MEDIA command generates a default file name by appending the string `exec.cmds.media` to the IBM Spectrum Protect server directory. The server directory is the current working directory of the IBM Spectrum Protect server process.

Windows If you do not specify a file name, the MOVE MEDIA command generates a default file name by appending the string *`exec.cmd.media`* to the IBM Spectrum Protect server directory. The server directory is the current working directory of the IBM Spectrum Protect server process.

The MOVE MEDIA command automatically allocates the file name that is specified or generated. If the file name exists, you can use the APPEND=YES parameter to add to the file. Otherwise, the file is overwritten. If a file is accidentally overwritten and you must run the commands that were in the file, issue the QUERY MEDIA command to rebuild the executable commands for the desired volumes. If the MOVE MEDIA command fails after the command file is allocated, the file is not deleted.

APPend
Specifies to write at the beginning or ending of the command file data. The default is NO. Possible values are:

No
Specifies to write the data from the beginning of the command file. If the command file exists, its contents are overwritten.
Yes
Specifies to append the command file by writing at the end of the command file data.

CHECKLabel
Specifies whether the server reads volume labels for sequential media. For SCSI devices, you can suppress label checking by setting the CHECKLabel to NO. This parameter is not applicable to 349X libraries. This parameter is optional. The default is YES. Possible values are:

Yes
Specifies that the server attempts to read the media label. Reading the media label verifies that the correct volume is being checked out.
No
Specifies that the server does not attempt to read media label. This increases performance because the read process does not occur.

CAP
Specifies which cartridge access port (CAP) to use for ejecting volumes if you specify REMOVE=YES. This parameter applies to volumes in ACSLS libraries only. If the CAP priority value is set to 0 in the library, this parameter is required. If a CAP priority value greater than 0 is set in the library, this parameter is optional. By default, all CAPs initially have a priority value of 0, which means that ACSLS does not automatically select the CAP.
To display valid CAP identifiers (*x,y,z*), issue the QUERY CAP command with ALL specified from the Automated Cartridge System System Administrator (ACSSA) console on the ACSLS server host. The identifiers are as follows:

x
The Automated Cartridge System (ACS) ID. This identifier can be a number in the range 0 - 126.
y
The Library Storage Module (LSM) ID. This identifier can be a number in the range 0 - 23.
z
The CAP ID. This identifier can be a number in the range 0 - 11.

For more information, see the StorageTek documentation.

Example: Move all full volumes out of the library

Move all full volumes that are in the ARCHIVE sequential primary storage pool out of the library.

```
move media * stgpool=archive
```

Example: Generate the checkin commands

Generate the CHECKIN LIBVOLUME commands for full and partially full volumes that are in the ONSITE.ARCHIVE primary storage pool and stored in the overflow location, Room 2948/Bldg31.

AIX Linux MOVE MEDIA creates the executable commands in /tsm/move/media/checkin.vols

Windows MOVE MEDIA creates the executable commands in c:\tsm\move\media\checkin.vols

```
move media * stgpool=onsite.archive
wherestate=mountablenotinlib wherestatus=full,filling
ovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols

checkin libvolume lib3494 TAPE04 status=private
checkin libvolume lib3494 TAPE13 status=private
checkin libvolume lib3494 TAPE14 status=private
```

Tip: Run the CHECKIN LIBVOLUME commands by issuing the MACRO command with the following as the macro name:

- AIX Linux /tsm/move/media/checkin.vols
- Windows c:\tsm\move\media\checkin.vols

Related commands

Table 5. Commands related to MOVE MEDIA

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY MEDIA	Displays information about storage pool volumes moved by the MOVE MEDIA command.
QUERY PROCESS	Displays information about background processes.

MOVE NODEDATA (Move data by node in a sequential access storage pool)

Use this command to move data that is in a sequential-access storage pool. You can move data for one or more nodes, a group of file spaces, or for a group of collocated nodes. You can also move selected file spaces for a single node. The data can be in a primary storage pool, a copy storage pool, or an active-data pool.

This command is helpful for reducing the number of volume mounts during client restore or retrieve operations by consolidating data for a specific node within a storage pool, or to move data to another storage pool. For example, you can use this command for moving data to a random-access storage pool in preparation for client restore processing.

Ensure that the access mode of the volumes from which you are moving the node data is read/write or read-only and that the access mode of the volumes to which you are moving the node data is set to read/write. This operation will not move data on volumes with access modes of offsite, unavailable, or destroyed.

The MOVE NODEDATA command takes two forms, depending on whether you are moving data only for selected filespaces. The syntax and parameters for each form are defined separately.

Restriction: You cannot move node data into or out of a storage pool that is defined with a CENTERA device class.

Table 1. Commands related to MOVE NODEDATA

Command	Description
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE DATA	Moves data from a specified storage pool volume to another storage pool volume.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY OCCUPANCY	Displays file space information by storage pool.
QUERY PROCESS	Displays information about background processes.
QUERY STGPOOL	Displays information about storage pools.
QUERY VOLUME	Displays information about storage pool volumes.
UPDATE COLLOCGROUP	Updates the description of a collocation group.

- MOVE NODEDATA (Move data in file spaces for one or more nodes or a collocation group)
  Use this command to move data in file spaces that belong to; one or more nodes, a node collocation group, or a file space collocation group.
- MOVE NODEDATA (Move data from selected file spaces of a single node)
  Use this command to move data for selected file spaces belonging to a single node.

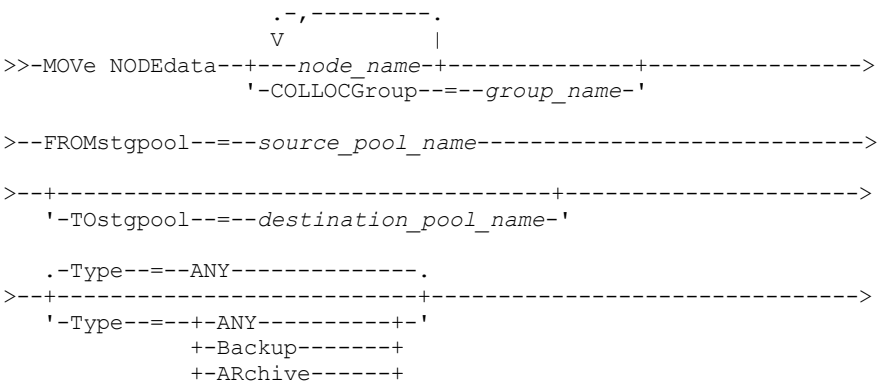
MOVE NODEDATA (Move data in file spaces for one or more nodes or a collocation group)

Use this command to move data in file spaces that belong to; one or more nodes, a node collocation group, or a file space collocation group.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the source storage pool. If your authorization is restricted storage privilege and you are moving data to another storage pool, you need the appropriate authority for the destination storage pool.

Syntax



```
              '-SPacemanaged-'

   .-MAXPRocess--=--1-------------.  .-Wait--=--No------.
>--+-----------------------------+--+------------------+------->
   '-MAXPRocess--=--num_processes-'  '-Wait--=--+-No--+-'
                                               '-Yes-'

                                (1)
   .-RECONStruct--=--No or Yes-----.
>--+-------------------------------+--------------------------><
   '-RECONStruct--=--+-No--+-------'
                     '-Yes-'
```

Notes:

1. The default is NO if either the source or target storage pool is random access. The default is YES if both the source and target storage pools are sequential access.

Parameters

node_name (Required unless the COLLOCGROUP parameter is specified)
: Specifies the node name that is related to the data that is moved with this command. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

COLLOCGroup (Required unless the node_name parameter is specified)
: Specifies the name of the collocation group whose data is to be moved. Data for all nodes and file spaces that belong to the collocation group are moved.

FROMstgpool (Required)
: Specifies the name of a sequential-access storage pool that contains data to be moved. This storage pool must be in the NATIVE or NONBLOCK data format.

TOstgpool
: Specifies the name of a storage pool to where the data is moved. This storage pool must be in the NATIVE or NONBLOCK data format. This parameter is optional and does not apply when the source storage pool is a copy storage pool or an active-data pool. That is, if the source storage pool is a copy storage pool the destination must be the same copy storage pool. Similarly, if the source storage pool is an active-data pool, the destination must be the same active-data pool. If a value is not specified, data is moved to other volumes within the source pool.
  Important: If you are moving data within the same storage pool, there must be volumes available that do not contain the node data that you are moving. That is, the server cannot use volumes that contain the data to be moved as destination volumes.

Type
: Specifies the type of files to be moved. This parameter is optional. The default value is ANY. If the source storage pool is an active-data pool, the only valid values are ANY and BACKUP. However, only the active versions of backup data are moved if TYPE=ANY. Specify one of the following values:

  ANY
  : Specifies that all types of files are moved.

  Backup
  : Specifies that backup files are moved.

  ARchive
  : Specifies that archive files are moved. This value is not valid for active-data pools.

  SPacemanaged
  : Specifies that space-managed files (files that were migrated by an IBM Spectrum Protect™ for Space Management client) are moved. This value is not valid for active-data pools.

MAXPRocess
: Specifies the maximum number of parallel processes to use for moving data. This parameter is optional. You can specify a value from 1 to 999, inclusive. The default value is 1. Increasing the number of parallel processes usually improves throughput.

  When you determine this value, consider the number of logical and physical drives that can be dedicated to this operation. To access a sequential access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect system activity. The mount points and drives also depend on the mount limits of the device classes for the sequential access storage pools that are involved in the move. Each process needs a mount point for storage pool volumes, and, if the device type is not FILE, each process also needs a drive.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is No. Specify one of the following values:

No

Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

The server displays messages that are created from the background process either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If a background process is canceled, some files might move before the cancellation.

Yes

Specifies that the server processes this command in the foreground. You wait for the command to complete before you can continue with other tasks. The server then displays the output messages to the administrative client when the command completes.
Restriction: You cannot specify WAIT=YES from the server console.

RECONStruct

Specifies whether to reconstruct file aggregates during data movement. Reconstruction removes empty space that accumulated during deletion of logical files from an aggregate. This parameter is optional. If both the source and target storage pools are sequential access, the default value is YES. If either the source or target storage pool is random access, the default is NO.
The parameter is not available or is ignored if any of the following conditions are true:

- The data format is NETAPPDUMP, CELERRADUMP, or NDMPDUMP.
- The data is in a storage pool that is configured for data deduplication.
- The target storage pool for the data movement is configured for data deduplication.

Attention: Reconstruction removes inactive backup files in active-data pools. If you specify RECONSTRUCT=NO when you move the data in an active-data pool that is not configured for data deduplication, inactive backup files remain in the storage pool.
You can specify one of the following values:

No

Specifies that reconstruction of file aggregates are not run during the move.

Yes

Specifies that reconstruction of file aggregates are run during the move. You can specify only this option when both the source and the target storage pools are sequential-access.

Move a specific node's data from a tape storage pool to a disk storage pool

Move all data that belongs to node MARY that is stored in storage pool TAPEPOOL. Data can be moved to disk storage pool BACKUPPOOL.

```
move nodedata mary
 fromstgpool=tapepool tostgpool=backuppool
```

Move data for a node collocation group from one storage pool to another

Move all data for node collocation group NODEGROUP1 from storage pool SOURCEPOOL to storage pool TARGETPOOL.

```
move nodedata collocgroup=nodegroup1 fromstgpool=sourcespool tostgpool=targetpool
```

Move data for a file space collocation group from one storage pool to another

Move all data for file space collocation group FSGROUP1 from storage pool SOURCEPOOL2 to storage pool TARGETPOOL2.

```
move nodedata collocgroup=fsgroup1 fromstgpool=sourcespool2 tostgpool=targetpool2
```

MOVE NODEDATA (Move data from selected file spaces of a single node)

Use this command to move data for selected file spaces belonging to a single node.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the source storage pool. If your authorization is restricted storage privilege and you intend to move data to another storage pool, you must also have the appropriate authority for the destination storage pool.

Syntax

Notes:

1. The default is NO if either the source or target storage pool is random access. The default is YES if both the source and target storage pools are sequential access.

Parameters

node_name (Required)
: Specifies the node name related to the data that is moved with this command. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names.

FROMstgpool (Required)
: Specifies the name of a sequential-access storage pool that contains data to be moved. This storage pool must be in the NATIVE or NONBLOCK data format.

TOstgpool
: Specifies the name of a storage pool to which data will be moved. This storage pool must be in the NATIVE or NONBLOCK data format. This parameter is optional and does not apply when the source storage pool is a copy storage pool or an active-data pool. That is, if the source storage pool is a copy storage pool the destination must be the same copy storage

pool. Similarly, if the source storage pool is an active-data pool, the destination must be the same active-data pool. If a value is not specified, data is moved to other volumes within the source pool.
Important: If you are moving data within the same storage pool, there must be volumes available that do not contain the node data you are moving. That is, the server cannot use volumes that contain the data to be moved as destination volumes.

FILespace
Specifies the name of the non-Unicode filespace that contains data to be moved. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. This parameter is optional. If you do not specify a value for this parameter and values for UNIFILESPACE or the FSID or both, non-Unicode file spaces are not moved.

UNIFILESpace
Specifies the name of the Unicode filespace that contains data to be moved. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. This parameter is optional. If you do not specify a value for this parameter and values for FILESPACE or the FSID or both, non-Unicode file spaces are not moved.

FSID
Specifies file space identifiers (FSIDs) for the file spaces to be moved. Separate multiple names with commas and no intervening spaces. This parameter is optional.

Type
Specifies the type of files to be moved. This parameter is optional. The default value is ANY. If the source storage pool is an active-data pool, the only valid values are ANY and BACKUP. However, only the active versions of backup data are moved if TYPE=ANY. Possible values are:

ANY
Specifies that all types of files are moved.

Backup
Specifies that backup files are moved.

ARchive
Specifies that archive files are moved. This value is not valid for active-data pools.

SPacemanaged
Specifies that space-managed files (files that were migrated by an IBM Spectrum Protect™ for Space Management client) are moved. This value is not valid for active-data pools.

MAXPRocess
Specifies the maximum number of parallel processes to use for moving data. This parameter is optional. You can specify a value from 1–999, inclusive. The default value is 1. Increasing the number of parallel processes should improve throughput.

When determining this value, consider the number of logical and physical drives that can be dedicated to this operation. To access a sequential access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the move. Each process needs a mount point for storage pool volumes, and, if the device type is not FILE, each process also needs a drive.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is No. Possible values are:

No
Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed.

The server displays messages that are created from the background process either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If a background process is canceled, some files may have already moved before the cancellation.

Yes
Specifies that the server processes this command in the foreground. You wait for the command to complete before continuing with other tasks. The server then displays the output messages to the administrative client when the command completes.
Restriction: You cannot specify WAIT=YES from the server console.

RECONStruct

Specifies whether to reconstruct file aggregates during data movement. Reconstruction removes empty space that has accumulated during deletion of logical files from an aggregate. This parameter is optional. If both the source and target storage pools are sequential access, the default value is YES. If either the source or target storage pool is random access, the default is NO.
The parameter is not available or is ignored if any of the following conditions are true:

- The data format is NETAPPDUMP, CELERRADUMP, or NDMPDUMP.
- The data is in a storage pool that is configured for data deduplication.
- The target storage pool for the data movement is configured for data deduplication.

Attention: Reconstruction removes inactive backup files in active-data pools. If you specify RECONSTRUCT=NO when moving the data in an active-data pool that is not configured for data deduplication, inactive backup files remain in the storage pool.
Possible values are:

No
: Specifies that reconstruction of file aggregates will not be performed during the move.

Yes
: Specifies that reconstruction of file aggregates will be performed during the move. You may only specify this option when both the source and the target storage pools are sequential-access.

Example: Move a node's non-Unicode and Unicode data

Move data for node TOM in storage pool TAPEPOOL. Restrict movement of data to files in non-Unicode file spaces as well as Unicode file spaces, \\jane\d$. Data should be moved to disk storage pool BACKUPPOOL.

```
move nodedata tom
 fromstgpool=tapepool tostgpool=backuppool
 filespace=* unifilespace=\\jane\d$
```

Example: Move all node data from tape storage pools to a disk storage pool

Move all data for node SARAH, from all primary sequential-access storage pools (for this example, TAPEPOOL*) to DISKPOOL. To obtain a list of storage pools that contain data for node SARAH, issue either of the following QUERY OCCUPANCY or SELECT commands:

```
query occupancy sarah
```

```
SELECT * from OCCUPANCY where node_name='sarah'
```

Attention: For this example assume that the results were TAPEPOOL1, TAPEPOOL4, and TAPEPOOL5.

```
move nodedata sarah
 fromstgpool=tapepool1 tostgpool=DISKPOOL

move nodedata sarah
 fromstgpool=tapepool4 tostgpool=DISKPOOL

move nodedata sarah
 fromstgpool=tapepool5 tostgpool=DISKPOOL
```

Example: Move a node's non-Unicode and Unicode file spaces

The following is an example of moving non-Unicode and Unicode file spaces for a node. For node NOAH move non-Unicode filespace \\servtuc\d$ and Unicode file space \\tsmserv1\e$ that has a filespace ID of 2 from sequential access storage pool TAPEPOOL to random access storage pool DISKPOOL.

```
move nodedata noah
 fromstgpool=tapepool tostgpool=diskpool
 filespace=\\tsmserv1\d$ fsid=2
```

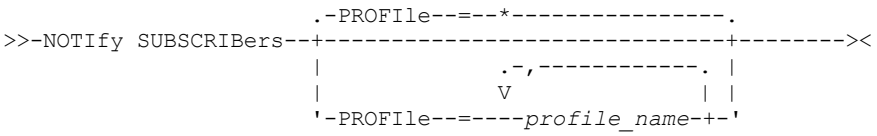
NOTIFY SUBSCRIBERS (Notify managed servers to update profiles)

Use this command on a configuration manager to notify one or more managed servers to request that their configuration information be immediately refreshed.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

PROFIle (Required)
: Specifies the name of the profile. Any managed servers that subscribe to the profile are notified. You can use wildcard characters to specify multiple profiles. To specify multiple profiles, separate the names with commas and no intervening spaces. The default is to notify all subscribers.

Example: Notify managed servers to update profiles

Notify all managed servers that subscribe to a profile named DELTA to request updated configuration information.

```
notify subscribers profile=delta
```

Related commands

Table 1. Commands related to NOTIFY SUBSCRIBERS

Command	Description
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
SET CONFIGREFRESH	Specifies a time interval for managed servers to contact configuration managers.

PERFORM LIBACTION (Define or delete all drives and paths for a library)

Use this command to define or delete all drives and their paths for a single library in one step.

This command can be used when you set up a library environment or modify an existing hardware setup that requires changes to many drive definitions. After you define a library, issue PERFORM LIBACTION to define drives and their paths for the library. You can also delete all drives and paths for a library by issuing the command with ACTION=DELETE.

This command is only valid for library types of SCSI and VTL. To use this command with ACTION=DEFINE, the SANDISCOVERY option must be supported and enabled.

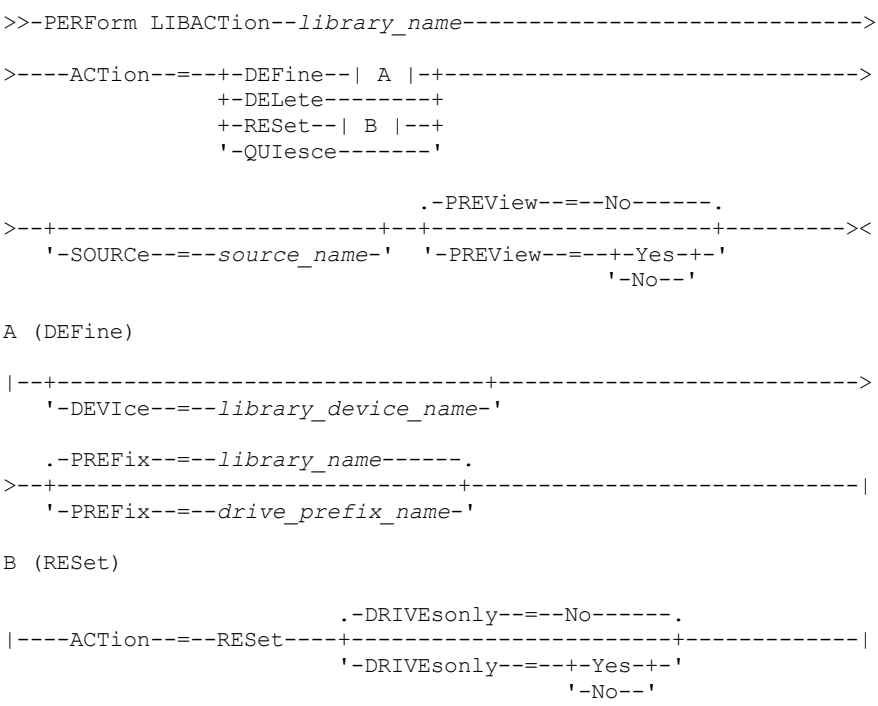
For detailed and current library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

library_name (Required)
: Specifies the name of the library to be defined or deleted. The maximum length of this name is 30 characters unless you are issuing PERFORM LIBACTION with ACTION=DEFINE and using the default PREFIX value. In that case, the maximum length of the name is 25 characters.

ACTion
: Specifies the action for the PERFORM LIBACTION command. Possible values are:

  DEFine
  : Specifies that drives and their paths are defined for the specified library. SAN discovery must be enabled before you specify this parameter value.

  DELete
  : Specifies that drives and their paths are deleted for the specified library.

  RESet
  : Specifies that drives and their paths are updated online for the specified library.

    DRIVEsonly
    : Specifies that only drives are updated online for the specified library.
      Possible values are:

      No
      : Specifies that drives and paths are updated online.

      Yes
      : Specifies that only drives are updated online.

  QUIesce
  : Specifies that drives are updated offline.

DEVIce
: Specifies the library device name that is used when you define paths if a path to the library is not already defined. If a path is already defined, the DEVICE parameter is ignored. The maximum length for this value is 64 characters. This parameter is optional.

PREFix

Specifies the prefix that is used for all drive definitions. For example, a PREFIX value of *DR* creates drives *DR0, DR1, DR2*, for as many drives as are created. If a value is not specified for the PREFIX parameter, the library name is used as the prefix for drive definitions. The maximum length for this value is 25 characters.

SOURCe

Specifies the source server name to be used when you define or delete drive path definitions on a library client or LAN-free client. Use this parameter only if the drives in the library are set up for the local server. If no value is specified for the SOURCE parameter, the local server name, which is the default, is used. The maximum length for the source name is 64 characters.

If you specify the SOURCE parameter, you can RESET only paths from specified SOURCE values. The SOURCE parameter is not compatible with the RESET DRIVESONLY=YES or QUIESCE options.

If a source name other than the local server name is specified with ACTION=DEFINE, drive path definitions are defined with the token value of UNDISCOVERED. The path definitions are then updated dynamically by library clients that support SAN Discovery the first time the drive is mounted.

PREView

Specifies the output of all commands that are processed for PERFORM LIBACTION before the command is issued. The PREVIEW parameter is not compatible with the DEVICE parameter. If you are issuing the PERFORM LIBACTION command to define a library, you cannot specify both the PREVIEW and the DEVICE parameter.
Possible values are:

No

Specifies that a preview of the commands that are issued for PERFORM LIBACTION is not displayed.

Yes

Specifies that a preview of the commands that are issued for PERFORM LIBACTION is displayed.

Example: Define a shared library

Assume that you are working in a SAN and that you configured a library manager named LIBMGR1. Now, define a library that is named SHAREDTSM to a library client server named LIBCL1.

Issue DEFINE LIBRARY from the library client server, LIBCL1:

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

Then, issue PERFORM LIBACTION from the library manager, LIBMGR1, to define the drive paths for the library client:

```
perform libaction sharedtsm action=define source=libcl1
```

Note: The SANDISCOVERY option must be supported and enabled on the library client server.

Example: Define a library with four drives

Define a SCSI library named KONA:

```
define library kona libtype=scsi
```

Then issue the PERFORM LIBACTION command to define drives and paths for the library:

AIX

```
perform libaction kona action=define device=/dev/lb3
prefix=dr
```

The server then runs the following commands:

```
define path server1 kona srct=server destt=library
device=/dev/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/mt3
define drive kona dr3
```

```
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/mt4
```

Linux

```
perform libaction kona action=define device=/dev/tsmscsi/lb3
prefix=dr
```

The server then runs the following commands:

```
define path server1 kona srct=server destt=library
device=/dev/tsmscsi/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt3
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt4
```

Windows

```
perform libaction kona action=define device=lb0.0.0.2
prefix=dr
```

The server then runs the following commands:

```
define path server1 kona srct=server destt=library
device=lb0.0.0.2
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=mt0.1.0.2
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=mt0.2.0.2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=mt0.3.0.2
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=mt0.4.0.2
```

Related commands

Table 1. Commands related to PERFORM LIBACTION

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE DRIVE	Deletes a drive from a library.
DELETE LIBRARY	Deletes a library.
DELETE PATH	Deletes a path from a source to a destination.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY PATH	Displays information about the path from a source to a destination.

Command	Description
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE LIBRARY	Changes the attributes of a library.
UPDATE PATH	Changes the attributes associated with a path.

PING SERVER (Test the connection between servers)

Use this command to test the connection between the local server and a remote server.

Important: The name and password of the administrator client issuing this command must also be defined on the remote server. If the remote server is at the current level, the server credentials are verified automatically when you run the PING SERVER command. If the remote server is not at the current level, the server credentials are not verified.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-PING SERVER--server_name-------------------------------------><
```

Parameters

server_name (Required)
Specifies the name of the remote server.

Example: Ping a server

Test the connection to server FRED.

```
ping server fred
```

Related commands

Table 1. Commands related to PING SERVER

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.
QUERY SERVER	Displays information about servers.

PREPARE (Create a recovery plan file)

Use this command to create a recovery plan file, which contains the information that is needed to recover an IBM Spectrum Protect™ server. You can store a recovery plan file on a file system that is accessible to the source server or on a target server.

You can use the QUERY ACTLOG command to view whether the PREPARE command was successful.

You can also view this information from the server console or, if the WAIT parameter equals YES, an administrative client session.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
.-Source--=--DBBackup-------.
```

Parameters

Source

Specifies the type of database backup series that IBM Spectrum Protect assumes when generating the recovery plan file. This parameter is optional. The default is DBBACKUP. The choices are:

DBBackup

Specifies that IBM Spectrum Protect assumes the latest full database backup series.

DBSnapshot

Specifies that IBM Spectrum Protect assumes the latest database snapshot backup series.

DEVclass

Specifies the device class name that is used to create a recovery plan file object on a target server. The device class must have a device type of SERVER.

Important: The maximum capacity for the device class must be larger than the size of the recovery plan file. If the size of the recovery plan file exceeds the maximum capacity, the command fails.

The naming convention for the archive object that contains the recovery plan file on the target server is:

- **Filespace name:**
  - ADSM.SERVER
- **High-level qualifier:**
  - AIX Linux devclassprefix/servername.yyyymmdd.hhmmss
  - Windows devclassprefix\servername.yyyymmdd.hhmmss
- **Low-level qualifier:**
  - RPF.OBJ.1

The recovery plan file virtual volume name as recorded in the volume history table on the source server is in the format `servername.yyyymmdd.hhmmss`.

If the DEVCLASS parameter is not specified, the recovery plan file is written to a file based on the plan prefix.

If SOURCE=DBBACKUP is specified or is defaulted to, the volume history entry for the recovery plan file object specifies a volume type of RPFILE. If SOURCE=DBSNAPSHOT is specified, the volume history entry specifies a volume type of RPFSNAPSHOT.

PLANPrefix

Specifies the path name prefix that is used in the recovery plan file name. This parameter is optional.

- AIX Linux The maximum length is 250 characters.
- Windows The maximum length is 200 characters.

Windows Specifies the path name prefix that is used in the recovery plan file name.

IBM Spectrum Protect appends to the prefix the sortable date and time format `yyyymmdd.hhmmss`. For example: 20081115.051421.

AIX Linux The prefix can be one of the following:

Directory path
: End the prefix with the forward slash (/). For example:

```
PLANPREFIX=/adsmsrv/recplans/
```

: The resulting file name would look like this:

```
/adsmsrv/recplans/20081115.051421
```

Directory path followed by a string
: IBM Spectrum Protect treats the string as part of the file name. For example:

```
PLANPREFIX=/adsmsrv/recplans/accounting
```

: The resulting file name looks like this:

```
/adsmsrv/recplans/accounting.20081115.051421
```

: Note the period before the date and time.

String only
: IBM Spectrum Protect specifies the directory path. IBM Spectrum Protect uses the name of the current working directory. For example, the current working directory is /opt/tivoli/tsm/server/bin and you specify the following parameter:

```
PLANPREFIX=shipping
```

: The resulting file name looks like this:

```
/opt/tivoli/tsm/server/bin/shipping.20081115.051421
```

: Note the period before the date and time.

Windows The prefix can be one of the following:

Directory path
: End the prefix with the back slash (\). For example:

```
PLANPREFIX=c:\adsmsrv\recplans\
```

: The resulting file name looks like this:

```
c:\adsmsrv\recplans\20081115.051421
```

: Tip: If you issue the PREPARE command from the administrative command line client and the last character in the command line is a back slash, it is interpreted as a continuation character. To avoid this, place the prefix value in double quotation marks. For example:

```
PLANPREFIX="c:\adsmsrv\recplans\"
```

Directory path followed by a string
: IBM Spectrum Protect treats the string as part of the file name. For example:

```
PLANPREFIX=c:\adsmsrv\recplans\accounting
```

: The resulting file name looks like this:

```
c:\adsmsrv\recplans\accounting.20081115.051421
```

: Note the period before the date and time.

String only
: IBM Spectrum Protect appends the date and time in the *.yyyymmdd.hhmmss* format (note the period before the date and time) to the prefix. The directory path used by the PREPARE command is the directory representing this “instance” of the IBM Spectrum Protect server. Typically, this directory is the original IBM Spectrum Protect server

installation directory. For example, the directory representing this instance of the server is c:\Program Files\Tivoli\TSM;\server2 , and you issue a PREPARE command with the following parameter:

```
PLANPREFIX=shipping
```

The resulting recovery plan filename is:

```
c:\Program Files\Tivoli\TSM;\server2\shipping.20081115.051421
```

If the PLANPREFIX parameter is not specified, IBM Spectrum Protect selects the prefix in one of these ways:

- If the SET DRMPLANPREFIX command has been issued, IBM Spectrum Protect uses the prefix specified in that command.
- Windows If the SET DRMPLANPREFIX command is not defined, IBM Spectrum Protect uses as the path the directory representing this “instance” of the IBM Spectrum Protect server, which is typically the original IBM Spectrum Protect server installation directory. For example, the directory representing this instance of the server is the following:

  ```
  c:\Program Files\Tivoli\TSM;\server2
  ```

  The resulting recovery plan file name is the following:

  ```
  c:\Program Files\Tivoli\TSM;\server2\2008115.051421
  ```

- AIX Linux If the SET DRMPLANPREFIX command has not been issued, IBM Spectrum Protect uses the directory path name of the current working directory. For example, the current working directory is the following:

  ```
  /opt/tivoli/tsm/server/bin
  ```

  The resulting file name looks like this:

  ```
  /opt/tivoli/txm/server/bin/20081115.051421
  ```

INSTRPrefix
: Specifies the prefix of the path name used by IBM Spectrum Protect to locate the files that contain the recovery instructions. The maximum length is AIX Linux 250 Windows 200 characters.
AIX Linux The prefix can be one of the following:

  Directory path
  : End the prefix with the forward slash (/). For example:

    ```
    INSTRPREFIX=/adsmsrv/recinstr/
    ```

    ```
    /adsmsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
    ```

  Directory path followed by a string
  : IBM Spectrum Protect treats the string as part of the file name. For example:

    ```
    INSTRPREFIX=/adsmsrv/recinstr/accounts
    ```

    IBM Spectrum Protect appends the appropriate recovery plan file stanza name. For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name is:

    ```
    /adsmsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
    ```

  String only
  : - IBM Spectrum Protect specifies the directory path and appends the appropriate recovery plan file stanza name. IBM Spectrum Protect uses the name of the current working directory. For example, the current working directory is /opt/tivoli/tsm/server/bin and you specify the following parameter:

      ```
      INSTRPREFIX=shipping
      ```

      For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name looks like this:

      ```
      /opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
      ```

  Windows The prefix can be one of the following:

  Directory path
  : End the prefix with the back slash (\). For example:

```
INSTRPREFIX=c:\adsmsrv\recinstr\
```

IBM Spectrum Protect appends the appropriate recovery plan file stanza name. For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name is:

```
c:\adsmsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

Tip: If you issue the PREPARE command from the administrative command line client and the last character in the command line is a back slash, it is interpreted as a continuation character. To avoid this, place the prefix value in double quotation marks. For example:

```
INSTRPREFIX="c:\adsmserv\recinstr\"
```

Directory path followed by a string
IBM Spectrum Protect treats the string as part of the file name. For example:

```
INSTRPREFIX=c:\adsmsrv\recinstr\accounts
```

IBM Spectrum Protect appends the appropriate recovery plan file stanza name. For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name is:

```
c:\adsmsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

String only
IBM Spectrum Protect specifies the directory path and appends the appropriate recovery plan file stanza name. IBM Spectrum Protect appends the recovery plan file stanza name to the prefix. If the prefix is only a string, the directory path used by the PREPARE command is the directory representing this instance of the IBM Spectrum Protect server. This is typically the original IBM Spectrum Protect server installation directory. For example, the directory representing this instance of the server is c:\Program Files\Tivoli\TSM;\server2, and you issue a PREPARE command with the following parameter:

```
INSTRPREFIX=dock
```

The resulting recovery plan filename is:

```
c:\Program Files\Tivoli\TSM;\server2\shipping.20081115.051421
```

If you do not specify the INSTRPREFIX parameter, IBM Spectrum Protect selects the prefix in one of these ways:

- If the SET DRMINSTRPREFIX command has been issued, IBM Spectrum Protect uses the prefix specified in that command.
- Windows If the SET DRMINSTRPREFIX command has not been issued, IBM Spectrum Protect uses as the path the directory representing this “instance” of the IBM Spectrum Protect server, which is typically the original server installation directory. For example, the directory representing this instance of the server is the following:

  ```
  c:\Program Files\Tivoli\TSM;\server2
  ```

  The resulting recovery plan file name is the following:

  ```
  c:\Program Files\Tivoli\TSM;\server2\RECOVERY.INSTRUCTIONS.GENERAL
  ```

- AIX Linux If the SET DRMINSTRPREFIX command has not been issued, IBM Spectrum Protect uses the current working directory.
  For example, if the current working directory is /opt/tivoli/tsm/server/bin, for the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would be:

  ```
  /opt/tivoli/tsm/server/bin/RECOVERY.INSTRUCTIONS.GENERAL
  ```

PRIMstgpool
Specifies the names of the primary storage pools that you want to restore. Separate the storage pool names with commas and no intervening spaces. You can use wildcard characters. If this parameter is not specified, IBM Spectrum Protect selects the storage pools as follows:

- If the SET DRMPRIMSTGPOOL command has been issued, IBM Spectrum Protect includes the primary storage pools named in that command.
- If the SET DRMPRIMSTGPOOL command has not been issued, IBM Spectrum Protect includes all the primary storage pools.

COPYstgpool

Specifies the names of the copy storage pools used to back up the primary storage pools that you want to restore (see the PRIMSTGPOOL parameter). Separate storage pool names with commas and no intervening spaces. You can use wildcard characters. If this parameter is not specified, IBM Spectrum Protect selects the storage pools as follows:

- If the SET DRMCOPYSTGPOOL command has been issued, IBM Spectrum Protect includes those copy storage pools.
- If the SET DRMCOPYSTGPOOL command has not been issued, IBM Spectrum Protect includes all copy storage pools.

ACTIVEDatastgpool
Specifies the names of the active-data storage pools that you want to have available for offsite access. Separate active-data storage-pool names with commas and no intervening spaces. You can use wildcard characters. If this parameter is not specified, IBM Spectrum Protect selects the storage pools as follows:

- If the SET ACTIVEDATASTGPOOL command has been previously issued with valid active-data storage pool names, IBM Spectrum Protect processes those storage pools.
- If the SET ACTIVEDATASTGPOOL command has not been issued, or all of the active-data storage pools have been removed using the SET ACTIVEDATASTGPOOL command, IBM Spectrum Protect processes only the active-data pool volumes that were marked on-site at the time the PREPARE command is run. IBM Spectrum Protect will mark these volumes as UNAVAILABLE.

Wait
Specifies whether this command is processed in the background or foreground.

No
Specifies background processing. This is the default.

Yes
Specifies foreground processing.

AIX Linux You cannot specify YES from the server console.

Example: Create a recovery plan file

Issue the PREPARE command and query the activity log to check the results.

```
prepare
query actlog search=prepare
```

AIX Linux

```
05/03/2008 12:01:13  ANR0984I Process 3 for PREPARE started in the
                      BACKGROUND at 12:01:13.
05/03/2008 12:01:13  ANR6918W PREPARE: Recovery instructions file
                      /home/guest/drmtest/prepare/tservr/DSM1509/
                      RECOVERY.INSTRUCTIONS.DATABASE not found.
05/03/2008 12:01:13  ANR6918W PREPARE: Recovery instructions file
                      /home/guest/drmtest/prepare/tservr/DSM1509/
                      RECOVERY.INSTRUCTIONS.STGPOOL not found.
05/03/2008 12:01:13  ANR6913W PREPARE: No volumes with backup data
                      exist in copy storage pool CSTORAGEP.
05/03/2008 12:01:13  ANR6913W PREPARE: No volumes with backup data
                      exist in copy storage pool CSTORAGEPSM.
05/03/2008 12:01:14  ANR6920W PREPARE: Generated replacement volume
                      name BACK4X@ is not valid for device type
                      8MM. Original volume name: BACK4X. Stanza is
                      PRIMARY.VOLUMES.REPLACEMENT macro.
05/03/2008 12:01:14  ANR6900I PREPARE: The recovery plan file
                      /home/guest/drmtest/prepare/plandir/DSM1509/
                      r.p.20080503.120113 was created.
05/03/2008 12:01:14  ANR0985I Process 3 for PREPARE running in the
                      BACKGROUND completed with completion state
                      SUCCESS at 12:01:14.
```

Windows

```
05/03/2008 12:01:13  ANR0984I Process 3 for PREPARE started in the
                      BACKGROUND at 12:01:13.
05/03/2008 12:01:13  ANR6918W PREPARE: Recovery instructions file
                      c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.DATABASE
                      not found.
05/03/2008 12:01:13  ANR6918W PREPARE: Recovery instructions file
                      c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.STGPOOL
```

```
                      not found.
05/03/2008 12:01:13   ANR6913W PREPARE: No volumes with backup data
                       exist in copy storage pool CSTORAGEP.
05/03/2008 12:01:13   ANR6913W PREPARE: No volumes with backup data
                       exist in copy storage pool CSTORAGEPSM.
05/03/2008 12:01:14   ANR6920W PREPARE: Generated replacement volume
                       name BACK4X@ is not valid for device class 8MM.
                       Original volume name: BACK4X. Stanza is
                       PRIMARY.VOLUMES.REPLACEMENT macro.
05/03/2008 12:01:14   ANR6900I PREPARE: The recovery plan file
                       c:\drmtest\prepare\r.p.20080503.120113
                       was created.
05/03/2008 12:01:14   ANR0985I Process 3 for PREPARE running in the
                       BACKGROUND completed with completion state
                       SUCCESS at 12:01:14.
```

Related commands

Table 1. Commands related to PREPARE

Command	Description
CANCEL PROCESS	Cancels a background server process.
DELETE VOLHISTORY	Removes sequential volume history information from the volume history file.
QUERY DRMSTATUS	Displays DRM system parameters.
QUERY RPFCONTENT	Displays the contents of a recovery plan file.
QUERY RPFILE	Displays information about recovery plan files.
QUERY SERVER	Displays information about servers.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
SET DRMACTIVEDATASTGPOOL	Specifies that active-data storage pools are managed by DRM.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.
SET DRMINSTRPREFIX	Specifies the prefix portion of the path name for the recovery plan instructions.
SET DRMPLANVPOSTFIX	Specifies the replacement volume names in the recovery plan file.
SET DRMPLANPREFIX	Specifies the prefix portion of the path name for the recovery plan.
SET DRMPRIMSTGPOOL	Specifies that primary storage pools are managed by DRM.
SET DRMRPFEXPIREDAYS	Set criteria for recovery plan file expiration.
UPDATE VOLHISTORY	Adds or changes location information for a volume in the volume history file.

AIX | Linux | Windows

PROTECT STGPOOL (Protect data that belongs to a storage pool)

Use this command to protect data in a directory-container storage pool by storing a copy of the data in another storage pool on a replication target server or on the same server by protecting the data to tape. When you protect the directory-container storage pool, you can later try to repair damage in the storage pool by using the REPAIR STGPOOL command.

When you issue the PROTECT STGPOOL command for a directory-container storage pool, data that is stored in that storage pool is backed up to the target that you specify. The data can be backed up to the following target types:

- A directory-container storage pool on the target replication server.
  Prerequisite: For the storage pool that is being protected, you must specify the target pool by using the PROTECTSTGPOOL parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.

When you regularly use the PROTECT STGPOOL command, you can typically reduce the processing time for the REPLICATE NODE command. The data extents that are already copied to the target replication server by storage pool protection operations are skipped when node replication is started.

As part of the PROTECT STGPOOL operation, processes might run to repair damaged extents in the target server's storage pool. The repair operation occurs under the following conditions:

- Both the source server and the target server must be at V7.1.5 or later.
- Extents that are already marked as damaged on the target server are repaired. The repair process does not run an audit process to identify damage.
- Only target extents that match source extents are repaired. Target extents that are damaged but have no match on the source server are not repaired.

Limitations: The repair operation that runs as part of the PROTECT STGPOOL operation has the following limitations:

- Extents that belong to objects that were encrypted are not repaired.
- The timing of the occurrence of damage on the target storage pool and the sequence of REPLICATE NODE and PROTECT STGPOOL commands can affect whether the repair process is successful. Some extents that were stored in the target storage pool by a REPLICATE NODE command might not be repaired.

- Container-copy storage pools on the same server, protected to tape.
  Prerequisite: For the storage pool that is being protected, you must specify the target storage pool by using the PROTECTLOCALSTGPOOLS parameter. For details about the parameter, see the commands for defining and updating directory-container storage pools (DEFINE STGPOOL and UPDATE STGPOOL commands).

  As part of the PROTECT STGPOOL operation, volumes in the target pool might be reclaimed. The value of the RECLAIM parameter for the container-copy storage pool affects whether volumes are reclaimed. For details about the parameter, see the commands for defining and updating container-copy storage pools (DEFINE STGPOOL and UPDATE STGPOOL commands).

Restriction: You cannot schedule multiple PROTECT STGPOOL operations to run concurrently. Wait for one PROTECT STGPOOL operation to finish before you start another.

Privilege class

To issue this command, you must have system privilege.

Syntax when the target is the replication server

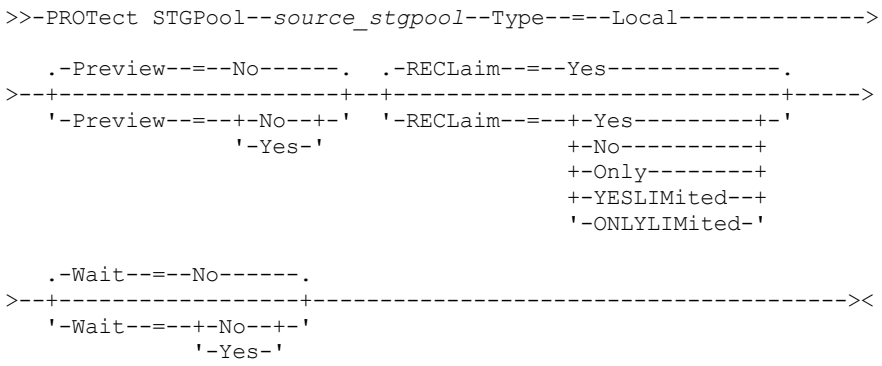
Notes:

1. Linux If the TRANSFERMETHOD parameter is set to the default value of TCPIP, the default value of the MAXSESSIONS parameter is 10. If the TRANSFERMETHOD parameter is set to FASP, the default value of the MAXSESSIONS parameter is

2.

2. Linux The TRANSFERMETHOD parameter is available only on Linux x86_64 operating systems.

Syntax when the target is a tape storage pool on the same server



Parameters

source_stgpool (Required)
: Specifies the name of the directory-container storage pool on the source server.

Type
: Specifies the type of target for the protection operation. This parameter is optional. The default value is REPLSERVER. Specify one of the following values:

  Replserver
  : Specifies that the target is the storage pool on the replication target server, as defined for the source storage pool with the PROTECTSTGPOOL parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.

  Local
  : Specifies that the target is on the same server as the source storage pool. The target is the container-copy storage pool that is defined for the source storage pool with the PROTECTLOCALSTGPOOLS parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.
  Tip: By default, the server uses a maximum of two parallel processes to copy data to a local target. You can change the maximum number of parallel processes by updating the container-copy storage pool that is the target. Use the UPDATE STGPOOL command with the PROTECTPROCESS parameter.

FORCEREConcile
: Specifies whether to reconcile the differences between data extents in the directory-container storage pool on the source server and target server. This parameter is optional. The default value is NO. Specify one of the following values:

  No
  : Specifies that data backup does not compare all data extents in the directory-container storage pool on the source server with data extents on the target server. Instead, data backup tracks changes to the data extents on the source server since the last backup and synchronizes these changes on the target server.

  Yes
  : Specifies that data backup compares all data extents on the source server with data extents on the target server and synchronizes the data extents on the target server with the source server.

MAXSESSions
: Specifies the maximum number of data sessions that can send data to a target server. This parameter is optional. The value that you specify can be in the range 1 - 100.

  AIX Windows The default value is 10.

  Linux The default value varies:

  - If TRANSFERMETHOD=TCPIP, the default value of the MAXSESSIONS parameter is 10.
  - If TRANSFERMETHOD=FASP, the default value of the MAXSESSIONS parameter is 2.

  If you increase the number of sessions, you can improve throughput for the storage pool.

When you set a value for the MAXSESSIONS parameter, ensure that the available bandwidth and the processor capacity of the source and target servers are sufficient.

Tips:

- If you issue a QUERY SESSION command, the total number of sessions might exceed the number of data sessions. The difference is because of short control sessions that are used to query and set up operations.
- The number of sessions that are used for protection depends on the amount of data that is backed up. If you are backing up only a small amount of data, increasing the number of sessions provides no benefit.

Preview
Specifies whether to preview data. This parameter is optional. The default value is NO. Specify one of the following values:

No
Specifies that the data is backed up to the target server but that the data is not previewed.
Yes
Specifies that data is previewed but not backed up.

PURGEdata
Specifies that data extents are deleted from the target server. This parameter is optional. The default value is NO. You can specify one of the following values:

No
Specifies that data extents that were deleted from the source server are deleted from the target server. New data extents are sent from the source server.
All
Specifies that all data extents are deleted from the target server, except for data extents that are referenced by other data in the target storage pool.
Deleted
Specifies that data extents that were deleted from the source server are deleted from the target server. No new data extents are sent from the source server.

RECLaim
Specifies whether reclamation runs when the PROTECT STGPOOL command is processed. Reclamation runs on the local container-copy storage pool that is the target for the protection operation. This parameter is optional. The default value is YES. You can specify one of the following values:

Yes
Specifies that reclamation runs when the command is issued, along with the storage pool protection operation. Reclamation runs to completion, with no limitation on the number of volumes in the storage pool that are processed for reclamation.
No
Specifies that reclamation is not run when the command is issued. Only the storage pool protection operation runs.
Only
Specifies that reclamation is the only operation that runs when the command is issued. The storage pool protection operation does not run, so data in the directory-container storage pool that was updated since the last protection operation is not protected. Reclamation runs to completion, with no limitation on the number of volumes in the storage pool that are processed for reclamation.
YESLIMited
Specifies that reclamation runs when the command is issued, along with the storage pool protection operation. Reclamation runs until it reaches the reclaim limit that is defined for the container-copy storage pool. The reclaim limit is defined with the RECLAIMLIMIT parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.
ONLYLIMited
Specifies that reclamation is the only operation that runs when the command is issued. The storage pool protection operation does not run, so data in the directory-container storage pool that was updated since the last protection operation is not protected. Reclamation runs until it reaches the reclaim limit that is defined for the container-copy storage pool. The reclaim limit is defined with the RECLAIMLIMIT parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.

Wait
Specifies whether to wait for the server to process this command in the foreground. This parameter is optional. The default value is NO. You can specify one of the following values:

No

Specifies that the command is processed in the background. To monitor the background processes of this command, issue the QUERY PROCESS command.

Yes

Specifies that the command is processed in the foreground. Messages are not displayed until the command completes processing.
Restriction: You cannot specify `WAIT=YES` from the server console.

Linux TRANSFERMethod

Linux Specifies the method that is used for server-to-server data transfer. This parameter is optional. You can specify one of the following values:

Tcpip

Specifies that TCP/IP is used to transfer data. This value is the default.

Fasp

Specifies that Aspera® Fast Adaptive Secure Protocol (FASP®) technology is used to transfer data. Aspera FASP technology can help you optimize data transfer in a wide area network (WAN). If you specify TRANSFERMETHOD=FASP, you override any TRANSFERMETHOD parameters that you specified on the DEFINE SERVER or UPDATE SERVER commands.
Restrictions:

- Before you enable Aspera FASP technology, determine whether the technology is appropriate for your system environment and install the appropriate licenses. For instructions, see Determining whether Aspera FASP technology can optimize data transfer in your system environment. If the licenses are missing or expired, operations to protect storage pools fail.
- If WAN performance meets your business needs, do not enable Aspera FASP technology.

Example: Delete all data extents from the target server

Delete all data extents in a directory-container storage pool on the target server. The directory-container storage pool that is named POOL1 on the source server is no longer protected by the directory-container storage pool on the target server. You might delete all extents to clean the directory-container storage pool on the target server that no longer protects the source server.

```
protect stgpool pool1 purgedata=all
```

Example: Protect a storage pool and specify a maximum number of data sessions

Protect a storage pool that is named SPOOL1 on the source server by backing up the data to a target replication server, TPOOL1. Specify a maximum of 20 data sessions.

```
update stgpool spool1 protectstgpool=tpool1
protect stgpool spool1 maxsessions=20
```

Example: Copy the storage pool data to tape

Protect a directory-container storage pool by copying the data to a container-copy storage pool on the same server. In this example, the directory-container storage pool is named SPOOL1 and the container-copy storage pool, which uses tape for storage, is named TAPES1.

1. Update the directory-container storage pool to add TAPES1 as the local storage pool for protection. The TAPES1 storage pool must be a container-copy storage pool. Issue the following command:

   ```
   update stgpool spool1 protectlocalstgpools=tapes1
   ```

2. Protect the data in the directory-container storage pool with a local copy by issuing the following command:

   ```
   protect stgpool type=local spool1
   ```

   The data is copied to the TAPES1 storage pool.

Example: Reclaim space on tape volumes before you protect a storage pool

Reclaim space on the tape volumes that are used to protect a directory-container storage pool. Then, protect the data in the directory-container storage pool. In this example, the directory-container storage pool is named SPOOL1.

1. Reclaim space in the local container-copy storage pool that is defined as the target protection pool for SPOOL1.

```
protect stgpool spool1 type=local reclaim=only
```

2. Protect the data in the directory-container storage pool that is named SPOOL1 without running reclamation.

```
protect stgpool spool1 type=local reclaim=no
```

Table 1. Commands related to PROTECT STGPOOL

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE STGPOOL (container-copy)	Define a container-copy storage pool that stores copies of data from a directory-container storage pool.
DEFINE STGPOOL (directory-container)	Define a directory-container storage pool.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
REPAIR STGPOOL	Repairs a directory-container storage pool.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET REPLSERVER	Specifies a target replication server.
UPDATE STGPOOL (container-copy)	Update a container-copy storage pool that stores copies of data from a directory-container storage pool.

QUERY commands

Use the QUERY commands to request or display information about IBM Spectrum Protect™ objects.

- QUERY ACTLOG (Query the activity log)
- QUERY ADMIN (Display administrator information)
- QUERY ALERTTRIGGER (Query the list of defined alert triggers)
- QUERY ALERTSTATUS (Query the status of an alert)
- QUERY ASSOCIATION (Query client node associations with a schedule)
- QUERY AUDITOCCUPANCY (Query client node storage utilization)
- QUERY BACKUPSET (Query a backup set)
- QUERY BACKUPSETCONTENTS (Query contents of a backup set)
- AIX Linux Windows QUERY CLEANUP (Query the cleanup that is required in a source storage pool)
- QUERY CLOPTSET (Query a client option set)
- QUERY COLLOCGROUP (Query a collocation group)
- QUERY CONTENT (Query the contents of a storage pool volume)
- AIX Linux Windows QUERY CONTAINER (Query a container)
- AIX Linux Windows QUERY CONVERSION (Query conversion status of a storage pool)
- QUERY COPYGROUP (Query copy groups)
- QUERY DATAMOVER (Display data mover definitions)
- AIX Linux Windows QUERY DAMAGED (Query damaged data in a directory-container or cloud-container storage pool)
- QUERY DB (Display database information)
- QUERY DBSPACE (Display database storage space)
- AIX Linux Windows QUERY DEDUPSTATS (Query data deduplication statistics)
- QUERY DEVCLASS (Display information on one or more device classes)
- QUERY DIRSPACE (Query storage utilization of FILE directories)
- QUERY DOMAIN (Query a policy domain)
- QUERY DRIVE (Query information about a drive)
- QUERY DRMEDIA (Query disaster recovery media)
- QUERY DRMSTATUS (Query disaster recovery manager system parameters)
- QUERY ENABLED (Query enabled events)
- QUERY EVENT (Query scheduled and completed events)
- QUERY EVENTRULES (Query rules for server or client events)
- QUERY EVENTSERVER (Query the event server)
- QUERY EXPORT (Query for active or suspended export operations)
- AIX Linux Windows QUERY EXTENTUPDATES (Query updated data extents)
- QUERY FILESPACE (Query one or more file spaces)

- QUERY LIBRARY (Query a library)
- QUERY LIBVOLUME (Query a library volume)
- QUERY LICENSE (Display license information)
- QUERY LOG (Display information about the recovery log)
- QUERY MACHINE (Query machine information)
- QUERY MEDIA (Query sequential-access storage pool media)
- QUERY MGMTCLASS (Query a management class)
- QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)
- QUERY MONITORSTATUS (Query the monitoring status)
- QUERY MOUNT (Display information on mounted sequential access volumes)
- AIX Linux Windows QUERY NASBACKUP (Query NAS backup images)
- QUERY NODE (Query nodes)
- QUERY NODEDATA (Query client data in volumes)
- QUERY NODEGROUP (Query a node group)
- QUERY OCCUPANCY (Query client file spaces in storage pools)
- QUERY OPTION (Query server options)
- QUERY PATH (Display a path definition)
- QUERY POLICYSET (Query a policy set)
- QUERY PROCESS (Query one or more server processes)
- QUERY PROFILE (Query a profile)
- QUERY PROTECTSTATUS (Query the status of storage pool protection)
- QUERY PROXYNODE (Query proxy authority for a client node)
- QUERY PVUESTIMATE (Display processor value unit estimate)
- QUERY RECOVERYMEDIA (Query recovery media)
- QUERY REPLICATION (Query node replication processes)
- QUERY REPLNODE (Display information about replication status for a client node)
- QUERY REPLRULE (Query replication rules)
- QUERY REPLSERVER (Query a replication server)
- QUERY REQUEST (Query one or more pending mount requests)
- QUERY RESTORE (Query restartable restore sessions)
- QUERY RPFCONTENT (Query recovery plan file contents stored on a target server)
- QUERY RPFILE (Query recovery plan file information stored on a target server)
- AIX Linux Windows QUERY SAN (Query the devices on the SAN)
- QUERY SCHEDULE (Query schedules)
- QUERY SCRIPT (Query IBM Spectrum Protect scripts)
- QUERY SERVER (Query a server)
- QUERY SERVERGROUP (Query a server group)
- QUERY SESSION (Query client sessions)
- QUERY SHREDSTATUS (Query shredding status)
- QUERY SPACETRIGGER (Query the space triggers)
- QUERY STATUS (Query system parameters)
- QUERY STATUSTHRESHOLD (Query status monitoring thresholds)
- QUERY STGRULE (Display storage rule information)
- QUERY STGPOOL (Query storage pools)
- AIX Linux Windows QUERY STGPOOLDIRECTORY (Query a storage pool directory)
- QUERY SUBSCRIBER (Display subscriber information)
- QUERY SUBSCRIPTION (Display subscription information)
- QUERY SYSTEM (Query the system configuration and capacity)
- AIX Linux Windows QUERY TAPEALERTMSG (Display status of SET TAPEALERTMSG command)
- AIX Linux Windows QUERY TOC (Display table of contents for a backup image)
- QUERY VIRTUALFSMAPPING (Query a virtual file space mapping)
- QUERY VOLHISTORY (Display sequential volume history information)
- QUERY VOLUME (Query storage pool volumes)

QUERY ACTLOG (Query the activity log)

Use this command to display messages generated by the server and client. This command provides filtering options that can be used to limit the number of messages displayed and the time that it takes to process this query. If you do not specify any parameters with this command, all messages generated in the previous hour are displayed.

The activity log contains all messages that are sent to the server console under normal operation. The results of commands entered at the server console are not recorded in the activity log unless the command affects or starts a background process or client session. Error messages are displayed in the activity log.

Restriction: You cannot schedule the QUERY ACTLOG command by using the DEFINE SCHEDULE command.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-BEGINDate--=--current_date-.
>>-Query ACtlog--+----------------------------+----------------><
                '-BEGINDate--=--date---------'

   .-BEGINTime--=--currenttime_minus_1_hour-.
>--+----------------------------------------+------------------><
   '-BEGINTime--=--time--------------------'

   .-ENDDate--=--current_date-.  .-ENDTime--=--current_time-.
>--+--------------------------+--+-------------------------+--->
   '-ENDDate--=--date---------'  '-ENDTime--=--time---------'

>--+--------------------------+--+-------------------+---------->
   '-MSGno--=--message_number-'  '-Search--=--string-'

>--+------------------------+-----------------------------------><
   '-NODEname--=--node_name-'

   .-ORiginator--=--ALL---------------.
>--+--------------------------------+-------------------------><
   '-ORiginator--=--+-ALL-----------+-'
                    +-SErver--------+
                    '-CLient--| A |-'

A

|--+------------------------+-------------------------------->
   '-OWNERname--=--owner_name-'

>--+----------------------------+------------------------------>
   '-SCHedname--=--schedule_name-'

>--+----------------------------+------------------------------>
   '-DOmainname--=--domain_name-'

>--+----------------------------+------------------------------|
   '-SESsnum--=--session_number-'
```

Parameters

BEGINDate

Specifies the beginning date of the range for messages to be displayed. All messages meeting the time range criteria that occurred after this date are displayed. The default is the current date. This parameter is optional.

You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –7 *or* –7. To display information beginning with messages created a week ago, you can specify BEGINDATE=TODAY-7 or BEGINDATE= -7.

Value	Description	Example
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time of the range for messages to be displayed. All messages meeting the time range criteria that occurred after this time are displayed. If you do not specify time, all messages that occurred in the last hour are displayed. You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	10:30:08
NOW	The current time on the specified begin date	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with BEGINTIME=NOW+3 or BEGINTIME=+3, IBM Spectrum Protect™ displays messages with a time of 12:00 or later on the begin date.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-04:00 *or* -04:00. If you issue the QUERY ACTLOG command at 9:00 with BEGINTime=NOW-3:30 or BEGINTime= -3:30, IBM Spectrum Protect displays messages with a time of 5:30 or later on the begin date.

ENDDate

Specifies the ending date of the range for messages to be displayed. All messages meeting the time range criteria that occurred before this date are displayed. If you do not specify a value, the current date is used. This parameter is optional. You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 *or* –1. To display information created up to yesterday, you can specify ENDDATE=TODAY-1 or simply ENDDATE= -1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time of the range for messages to be displayed. All messages meeting this time range criteria that occurred before this time are displayed. If you do not specify a value, all messages are displayed up to the time when you issued this command. This parameter is optional.

You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with ENDTIME=NOW+3:00 or ENDTIME= +3:00, IBM Spectrum Protect displays messages with a time of 12:00 or earlier on the end date you specify.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date	NOW-03:30 *or* -03:30. If you issue this command at 9:00 with ENDTIME=NOW-3:30 or ENDTIME= -3:30, IBM Spectrum Protect displays messages with a time of 5:30 or earlier on the end date you specify.

MSGno

Specifies an integer that defines the number of the message to be displayed from the activity log. This integer is just the numeric part of the message. This parameter is optional.

Search

Specifies a text string that you want to search for in the activity log. Enclose the string expression in quotation marks if it contains blanks. You can use text and a wildcard character to specify this string. This parameter is optional.

Note: Do not enter as a text string either the IBM Spectrum Protect server name or text and a wildcard character that would find the server name. If you do so, the output includes messages that do not include the search string.

NODEname

Specifies that the query displays messages logged for this node. If you do not specify a value for this parameter, messages for all nodes are displayed.

ORiginator

Specifies that the query displays messages logged by the server, client, or both. The default is ALL. Possible values are:

ALL

Specifies that the query displays messages that originated from the client and the server.

SErver

Specifies that the query displays messages that originated from the server.

CLient

Specifies that the query displays messages that originated from the client.

You can specify one of the following values to minimize processing time when querying the activity log for messages logged by the client:

OWNERname

Specifies that the query displays messages logged for a particular owner. If you do not specify a value for this parameter, messages for all owners are displayed.

SCHedname

Specifies that the query displays messages logged by a particular scheduled client activity. If you do not specify a value for this parameter, messages for all schedules are displayed.

DOmainname

Specifies that the query displays messages logged for a particular policy domain to which a named schedule belongs. This parameter is optional, unless you are specifying a schedule name.

SESsnum

Specifies that the query displays messages logged from a particular client session number. If you do not specify a value for this parameter, messages for all client sessions are displayed.

Example: Search activity log for messages with specific text

Search the activity log for any message that contains the string "delete". The output includes only messages produced during the past hour. Issue the command:

```
query actlog search=delete

Date/Time            Message
-------------------- ----------------------------------------
08/27/1998 15:19:43  ANR0812I Inventory client file expiration
                      complete: 0 files deleted.
```

Example: Search activity log for messages within a specific time frame

Display messages that occurred yesterday between 9:30 and 12:30. Issue the command:

```
query actlog begindate=today-1
begintime=09:30:00 endtime=12:30:00

Date/Time           Message
------------------- ---------------------------------------------
10/21/1998 10:52:36 ANR0407I Session 3921 started for administrator
                    ADMIN (WebBrowser) (HTTP 9.115.20.100(2315)).
10/21/1998 11:06:08 ANR0405I Session 3922 ended for administrator
                    ADMIN (WebBrowser).
10/21/1998 12:16:50 ANR0405I Session 3934 ended for administrator
                    ADMIN (WebBrowser).
```

Example: Search activity log for messages from a specific client node

Search the activity log for IBM Spectrum Protect messages from the client for node JEE. Issue the command:

```
query actlog originator=client node=jee

Date/Time           Message
------------------- -------------------------------------------------
06/10/1998 15:46:22 ANE4007E (Session No: 3 Node: JEE) Error
                    processing '/jee/report.out': access to the
                    object is denied
06/11/1998 15:56:56 ANE4009E (Session No: 4 Node: JEE) Error
                    processing '/jee/work.lst': disk full condition
```

Example: Search activity log for client and server messages from a specific client node and session

Search the activity log for IBM Spectrum Protect messages from the client and server for node A associated with Session 1. The output includes all messages with the defined text string, "SESSION: 1". Issue the command:

```
query actlog search="(SESSION:1)"

Date/Time            Message
-------------------  -------------------------------------------------
02/13/2012 12:13:42   ANR0406I Session 1 started for node A (WinNT)
                       (Tcp/Ip colind(2463)). (SESSION: 1)
02/13/2012 12:13:56  ANE4952I (ANE4985I Session: 1, ANE4986I Node: A)
                       Total number of objects inspected:       34
                       (SESSION: 1)
02/13/2012 12:13:56  ANE4954I (ANE4985I Session: 1, ANE4986I Node: A)
                       Total number of objects backed up:       34
                       (SESSION: 1)
02/13/2012 12:13:56  ANE4958I (ANE4985I Session: 1, ANE4986I Node: A)
                       Total number of objects updated:          0
                       (SESSION: 1)
02/13/2012 12:13:56  ANE4964I (ANE4985I Session: 1, ANE4986I Node: A)
                       Elapsed processing time:           00:00:02
                       (SESSION: 1)
```

```
02/13/2012 12:13:59  ANR0403I Session 1 ended for node A (WinNT).
                      (SESSION: 1)
```

Example: Search activity log for client-generated messages from a client session

Search the activity log for IBM Spectrum Protect messages from a specific client session. The output includes only messages generated by the client. Issue the command:

```
query actlog sessnum=1
```

```
Date/Time            Message
-------------------  ------------------------------------------------
02/13/2012 12:13:56  ANE4952I (ANE4985I Session: 1, ANE4986I Node: A)
                      Total number of objects inspected:       34
                      (SESSION: 1)
02/13/2012 12:13:56  ANE4954I (ANE4985I Session: 1, ANE4986I Node: A)
                      Total number of objects backed up:       34
                      (SESSION: 1)
02/13/2012 12:13:56  ANE4958I (ANE4985I Session: 1, ANE4986I Node: A)
                      Total number of objects updated:          0
                      (SESSION: 1)
02/13/2012 12:13:56  ANE4964I (ANE4985I Session: 1, ANE4986I Node: A)
                      Elapsed processing time:           00:00:02
                      (SESSION: 1)
```

Field descriptions

Date/Time
: Specifies the date and time when the message was generated by the server or client.

Message
: Specifies the message that was generated by the server or client.

Related commands

Table 1. Command related to QUERY ACTLOG

Command	Description
SET ACTLOGRETENTION	Specifies the number of days to retain log records in the activity log.

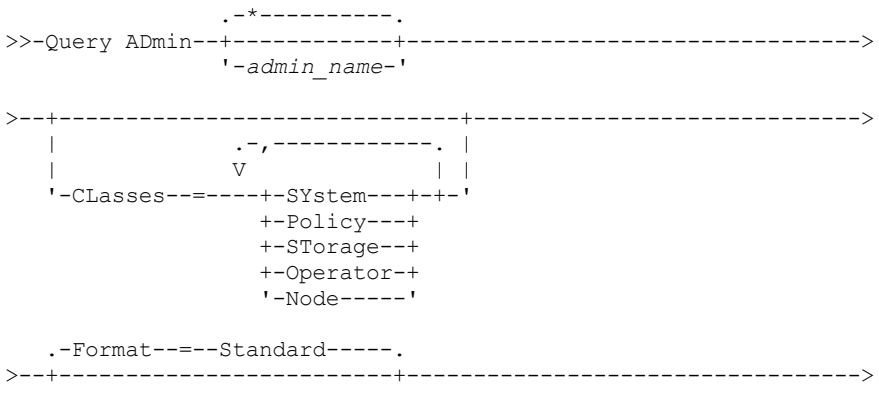
QUERY ADMIN (Display administrator information)

Use this command to display information about one or more administrators.

Privilege class

Any administrator can issue this command.

Syntax



```
   '-Format--=--+-Standard-+-'
                '-Detailed-'

>--+-----------------------------+--+--------------------+----><
   '-AUTHentication--=--+-LOcal-+-'  '-ALerts--=--+-Yes-+-'
                        '-LDap--'                 '-No--'
```

Parameters

admin_name
: Specifies the name of the administrator for which you want to display information. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, all administrators are displayed.

CLasses
: Specifies that you want to restrict output to those administrators that have privilege classes that you specify. This parameter is optional. You can specify multiple privilege classes in a list by separating the names with commas and no intervening spaces. If you do not specify a value for this parameter, information about all administrators is displayed, regardless of privilege class. Possible values are:

  SYstem
  : Display information on administrators with system privilege.

  Policy
  : Display information on administrators with policy privilege.

  STorage
  : Display information on administrators with storage privilege.

  Operator
  : Display information on administrators with operator privilege.

  Node
  : Display information on users with client node privilege.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the specified administrators.

  Detailed
  : Specifies that complete information is displayed for the specified administrators.

Authentication
: Specifies the password authentication method for the administrator.

  LOcal
  : Display those administrators authenticating to the IBM Spectrum Protect™ server.

  LDap
  : Display those administrators authenticating to an LDAP directory server. The administrator password is case-sensitive.

ALert
: Specifies whether alerts are sent to an administrators email address.

  Yes
  : Specifies that alerts are sent to the specified administrators email address.

  No
  : Specifies that alerts are not sent to the specified administrators email address. This is the default value.

  Tip: Alert monitoring must be enabled, and email settings must be correctly defined to successfully receive alerts by email. To view the current settings, issue the QUERY MONITORSETTINGS command.

Example: Display information about all administrators

Display partial information on all administrators. Issue the command:

```
query admin
```

```
Administrator   Days Since  Days Since   Locked?   Privilege Classes
Name           Last Access    Password
```

```
                                        Set
-------------  -----------  ----------  ---------  ------------------
ADMIN                   <1          <1         No  System
SERVER_CONSOLE                                 No  System
```

See Field descriptions for field descriptions.

Example: Display complete information about one administrator

From a managed server, display complete information for the administrator named ADMIN. Issue the command:

```
query admin admin format=detailed
```

```
        Administrator Name: ADMIN
     Last Access Date/Time: 1998.06.04 17.10.52
    Days Since Last Access: <1
    Password Set Date/Time: 1998.06.04 17.10.52
   Days Since Password Set: 26
     Invalid Sign-on Count: 0
                   Locked?: No
                   Contact:
          System Privilege: Yes
          Policy Privilege: **Included with system privilege**
         Storage Privilege: **Included with system privilege**
        Operator Privilege: **Included with system privilege**
   Client Access Privilege: **Included with system privilege**
    Client Owner Privilege: **Included with system privilege**
    Registration Date/Time: 05/09/1998 23:54:20
 Registering Administrator: SERVER_CONSOLE
          Managing profile:
Password Expiration Period: 90 Day (s)
             Email Address:
               Email Aerts: Yes
            Authentication: Local
              SSL Required: No
          Session Security: Strict
          Transport Method: TLS 1.2
```

See Field descriptions for field descriptions.

Field descriptions

Administrator Name
: Specifies the name of the administrator.

Last Access Date/Time
: Specifies the date and time that the administrator last accessed the server.

Days Since Last Access
: Specifies the number of days since the administrator last accessed the server.

Password Set Date/Time
: Specifies the date and time that the administrator's password was defined or most recently updated.

Days Since Password Set
: Specifies the number of days since the administrator's password was defined or most recently updated.

Invalid Sign-on Count
: Specifies the number of invalid sign-on attempts that have been made since the last successful sign-on. This count can only be non-zero when an invalid password limit (SET INVALIDPWLIMIT) is greater than zero. When the number of invalid attempts equals the limit set by the SET INVALIDPWLIMIT command, the administrator is locked out of the system.

Locked?
: Specifies whether the administrator is locked out of the system.

Contact
: Specifies any contact information for the administrator.

System Privilege
: Specifies whether the administrator has been granted system privilege.

Policy Privilege
: Specifies whether the administrator has been granted unrestricted policy privilege or the names of any policy domains that the restricted policy administrator can manage.

Storage Privilege

Specifies whether the administrator has been granted unrestricted storage privilege or the names of any storage pools that the restricted storage administrator can manage.

Operator Privilege
: Specifies whether the administrator has been granted operator privilege.

Client Access Privilege
: Specifies that client access authority has been granted to a user with node privilege.

Client Owner Privilege
: Specifies that client owner authority has been granted to a user with node privilege.

Registration Date/Time
: Specifies the date and time that the administrator was registered.

Registering Administrator
: Specifies the name of the administrator who registered the administrator. If this field contains $$CONFIG_MANAGER$$, the administrator is associated with a profile that is managed by the configuration manager.

Managing Profile
: Specifies the profiles to which the managed server subscribed to get the definition of this administrator.

Password Expiration Period
: Specifies the administrator's password expiration period.

Email Address
: Specifies the email address for the administrator.

Email Alerts
: Specifies whether alerts are sent to the specified administrator by email.

Authentication
: Specifies the password authentication method: LOCAL, LDAP, or LDAP (pending).

Authentication Target	**Authentication Method**
IBM Spectrum Protect server	LOCAL
LDAP directory server	LDAP
This administrator is configured to authenticate with an LDAP directory server, but the administrator did not yet authenticate through a client node.	LDAP (pending)

SSL Required (deprecated)
: Specifies whether the security setting for the administrator user ID requires the Secure Sockets Layer (SSL) protocol. Values can be YES, NO, or Default. You must have system level authority to update the administrator SSLREQUIRED setting. This parameter is deprecated.

Session Security
: Specifies the level of session security that is enforced for the administrator ID. Values can be STRICT or TRANSITIONAL.

Transport Method
: Specifies the transport method that was last used for the specified administrator. Values can be TLS 1.2, TLS 1.1, or NONE. A question mark (?) is displayed until a successful authentication is completed.

Related commands

Table 1. Commands related to QUERY ADMIN

Command	**Description**
GRANT AUTHORITY	Assigns privilege classes to an administrator.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
REMOVE ADMIN	Removes an administrator from the list of registered administrators.
RENAME ADMIN	Changes an IBM Spectrum Protect administrator’s name.
RESET PASSEXP	Resets the password expiration for nodes or administrators.

Command	Description
REVOKE AUTHORITY	Revokes one or more privilege classes or restricts access to policy domains and storage pools.
SET INVALIDPWLIMIT	Sets the number of invalid logon attempts before a node is locked.
SET MINPWLENGTH	Sets the minimum length for client passwords.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.

QUERY ALERTTRIGGER (Query the list of defined alert triggers)

Use this command to display which server messages are defined as alerts.

Privilege class

Any administrator can issue this command.

Syntax

```
                        .-*------------------.
>>-Query ALERTTrigger--+--------------------+------------------><
                        '---message_number---'
```

Parameters

message_number
: Specifies the message number that you want to query. Specify multiple message numbers, which are separated by commas, and no intervening spaces. Message numbers are a maximum of eight characters in length. Wildcard characters can be used to specify message numbers. If you do not specify a message number, all alert triggers are displayed.

Query alert triggers to display which messages are designated as alerts

Display all messages that are designated as alerts by issuing the following command:

```
query alerttrigger
```

Example output:

```
Alert Trigger        Category       Administrator
--------------       ---------      ------------------------------
ANR1067E             SERVER         HARRYH
ANR1073E             SERVER         CSDADMIN,DJADMIN,HARRYH
ANR1074E             STORAGE        CSDADMIN,DJADMIN,HARRYH
ANR1096E             STORAGE        CSDADMIN,DJADMIN,HARRYH,MHAYE
```

Query alert triggers for a specific message number

Display all alert triggers that have message number ANR1067E designated to them by issuing the following command:

```
query alerttrigger ANR1067E
```

Example output:

```
Alert Trigger        Category       Administrator
--------------       ---------      -------------
ANR1067E             SERVER         HARRYH
```

Field descriptions

Alert Trigger

The message number for the alert trigger.

Category

The category of the alert trigger.

Administrator

The name of the administrator who receives alerts from this alert trigger.

Related commands

Table 1. Commands related to QUERY ALERTTRIGGER

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

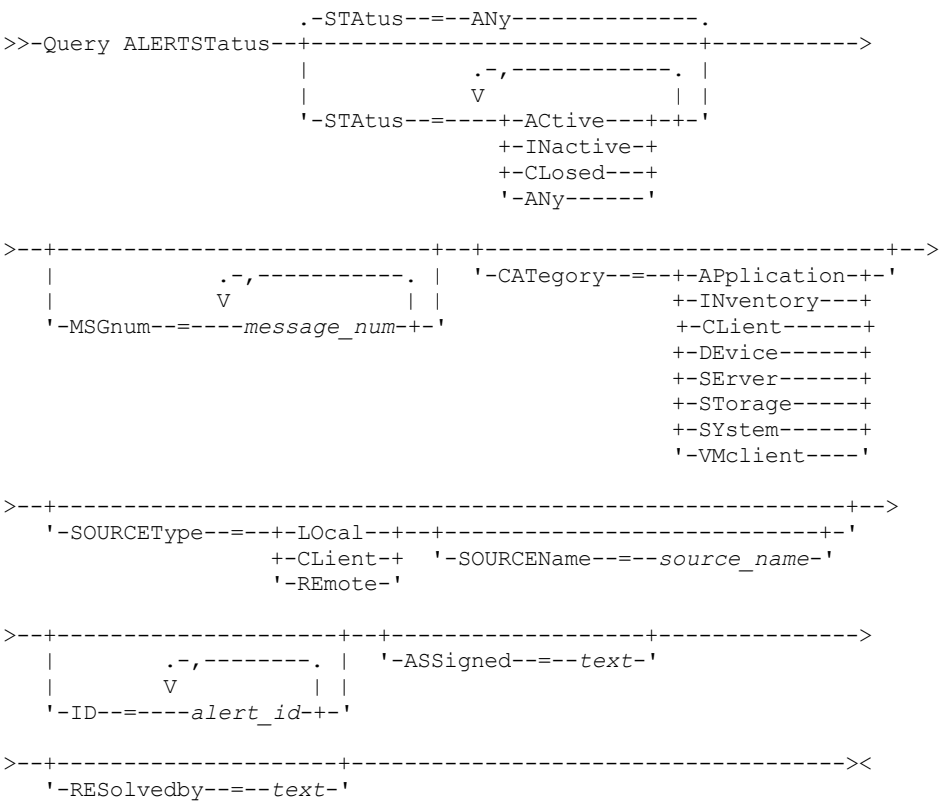
QUERY ALERTSTATUS (Query the status of an alert)

Use this command to display information about alerts that are reported on the IBM Spectrum Protect™ server.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

Status
Specifies the status type that you want to display. If you do not specify a status, all alerts are queried and displayed. Specify one of the following values:

ACtive
Displays alerts that are specified in the IBM Spectrum Protect server database as active.
INactive
Displays alerts that are in the inactive state.
CLosed
Displays alerts that are in the closed state.
ANy
Displays all alerts, without regard to state.

MSGnum
Specifies the message number that you want to display. Specify the numerical portion of an IBM Spectrum Protect server message. Values are in the range 0 - 9999. For example, the message number in message ANR2044E is 2044. Specify multiple message numbers by separating them with commas and no intervening spaces.

CATegory
Specifies the category type for the alert, which is determined by the message types. Specify one of the following values:

APplication
Alert is classified as application category. For example, you can specify this category for messages that are associated with application (TDP) clients.
INventory
Alert is classified as inventory category. For example, you can specify this category for messages that are associated with the database, active log file, or archive log file.
Note: The category of `CAtalog` is used instead of `INventory` in alerts from servers that were not upgraded to IBM Spectrum Protect 7.1.0 or later.
CLient
Alert is classified as client category. For example, you can specify this category for messages that are associated with general client activities.
DEvice
Alert is classified as device category. For example, you can specify this category for messages that are associated with device classes, libraries, drives, or paths.
SErver
Alert is classified as general server category. For example, you can specify this category for messages that are associated with general server activities or events.
STorage
Alert is classified as storage category. For example, you can specify this category for messages that are associated with storage pools.
SYstems
Alert is classified under system clients category. For example, you can specify this category for messages that are associated with system backup and archive or hierarchical storage management (HSM) backup-archive clients.
VMclient
Alert is classified under VMclient category. For example, you can specify this category for messages that are associated with virtual machine clients.

SOURCEType
Specifies the source type that is being queried. Specify one of the following values:

LOcal
Displays alerts that originated from the local IBM Spectrum Protect server.
CLient
Displays alerts that originated from the IBM Spectrum Protect client.
REmote
Displays alerts that originated from another IBM Spectrum Protect server.

SOURCEName
Specifies the name of the source where the alert originated. SOURCENAME can be the name of a local or remote IBM Spectrum Protect server, or an IBM Spectrum Protect client.

ID
This optional parameter specifies the unique ID of the alert that you want to display. Specify a value from 1 to 9223372036854775807.

ASSigned
Specifies the administrator name that is assigned the alert that you want to query.
RESolvedby
Specifies the administrator name that resolved the alert that you want to query.

Query active alerts

Display only alerts that are active in the server database by issuing the following command:

```
query alertstatus status=active
```

Query active alerts for two messages issued by the local server

Issue the following command to display only active alerts for message numbers ANE4958I and ANR4952E that were issued by the local server:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=local
```

Query active alerts for messages ANR4958I and ANR4952E issued by a client

Issue the following command to display only active alerts for message numbers ANE4958I and ANE4952I that were issued by a client:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=client
```

Query all alerts on a server

Issue the following command to display all alerts that are on the server:

```
query alertstatus
```

Example output: Display all the alerts that are on the server:

```
      Alert Identifier: 83
  Alert Message Number: 293
           Source Name: SEDONA
           Source Type: LOCAL
      First Occurrence: 03/07/2013 17:08:35
Most Recent Occurrence: 03/07/2013 17:08:35
                 Count: 1
                Status: ACTIVE
    Last Status Change: 12/31/1969 17:00:00
              Category: INVENTORY
               Message: ANR0293I Reorganization for table AF_BITFILES
                        started.
              Assigned:
           Resolved By:
                Remark:

      Alert Identifier: 85
  Alert Message Number: 293
           Source Name: SEDONA
           Source Type: LOCAL
      First Occurrence: 03/08/2013 05:45:00
Most Recent Occurrence: 03/08/2013 05:45:00
                 Count: 1
                Status: ACTIVE
    Last Status Change: 12/31/1969 17:00:00
              Category: INVENTORY
               Message: ANR0293I Reorganization for table
                        BF_AGGREGATED_BITFILES started.
              Assigned:
           Resolved By:
                Remark:

      Alert Identifier: 1282
  Alert Message Number: 293
           Source Name: ALPINE
           Source Type: LOCAL
      First Occurrence: 02/13/2013 15:47:50
```

```
Most Recent Occurrence: 02/13/2013 15:47:50
                 Count: 1
                Status: CLOSED
    Last Status Change: 02/26/2013 09:46:39
              Category: INVENTORY
               Message: ANR0293I Reorganization for table
                        TSMMON_ALERT started.
              Assigned:
           Resolved By:
                Remark:


      Alert Identifier: 1792
  Alert Message Number: 293
           Source Name: ALPINE
           Source Type: LOCAL
      First Occurrence: 02/19/2013 08:58:14
Most Recent Occurrence: 02/19/2013 08:58:14
                 Count: 1
                Status: CLOSED
    Last Status Change: 03/01/2013 12:39:21
              Category: INVENTORY
               Message: ANR0293I Reorganization for table
                        ACTIVITY_LOG started.
              Assigned:
           Resolved By:
                Remark:
```

Field descriptions

Alert Identifier
: The unique identifier for the alert.

Alert Message Number
: The message number for the alert.

Source Name
: The name of the source from where the alert originated.

Source Type
: The type of the originating source.

First Occurrence
: The date and time when the alert first occurred.

Most Recent Occurrence
: The date and time when the alert occurred last.

Count
: The total number of times the alert has been triggered.

Status
: Specifies the status of the alert.

Last Status Change
: Specifies the time and date when the status for the alert last changed.

Category
: The category for the alert.

Message
: The message that triggers the alert.

Assigned
: Specifies the user whom this alert concerns.

Resolved By
: Species the user who has investigated and resolved the alert.

Remark
: An optional remark to be left by the resolver.

Related commands

Table 1. Commands related to QUERY ALERTSTATUS

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.

Command	Description
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

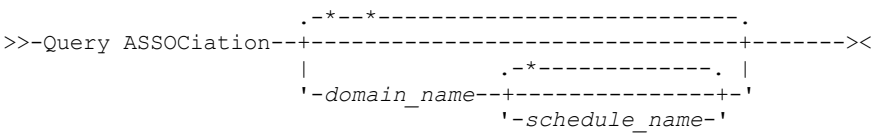
QUERY ASSOCIATION (Query client node associations with a schedule)

Use this command to display information about which client nodes are associated with one or more schedules. Client nodes associated with a schedule perform operations such as backup or archive according to that schedule.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

domain_name
: Specifies the name of the policy domain to display. You can use a wildcard character to specify this name. All matching policy domain names are displayed. If you do not specify a value for this parameter, all existing policy domains are queried. If you specify a domain name, you do not have to specify a schedule name.

schedule_name
: Specifies the name of the schedule to display. You can use a wildcard character to specify this name. All matching schedule names are displayed. If you do not specify a value for this parameter, all existing schedules are queried. If you specify a schedule name, you must also specify a policy domain name.

Example: Display client nodes that are associated with a schedule

Display all the client nodes that are associated with each schedule that belongs to the EMPLOYEE_RECORDS policy domain. Issue the command:

```
query association employee_records *

Policy Domain Name: EMPLOYEE_RECORDS
     Schedule Name: WEEKLY_BACKUP
  Associated Nodes: JOE JOHNSON LARRY SMITH SMITHERS TOM
```

See Field descriptions for field descriptions.

Field descriptions

Policy Domain Name
: Specifies the name of the policy domain to which the schedule belongs.

Schedule Name
: Specifies the name of the schedule.

Associated Nodes
: Specifies the names of the client nodes that are associated with the specified schedule.

Related commands

Table 1. Commands related to QUERY ASSOCIATION

Command	Description
DEFINE ASSOCIATION	Associates clients with a schedule.
DELETE ASSOCIATION	Deletes the association between clients and a schedule.

QUERY AUDITOCCUPANCY (Query client node storage utilization)

Use this command to display information about client node server storage utilization. To display current license audit information from the server, use the AUDIT LICENSE command before you issue the QUERY AUDITOCCUPANCY command.

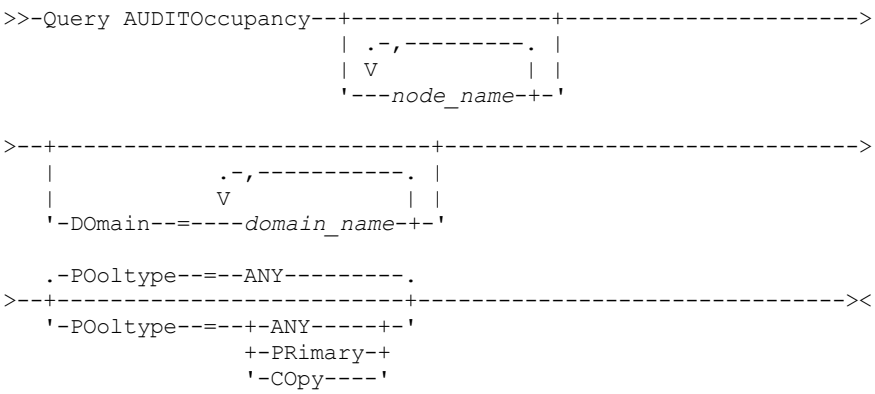
As part of a license audit operation, the server calculates, by node, the amount of backup, archive, and space management storage in use. For servers that manage large amounts of data, this calculation can take a great deal of processor time and can stall other server activity. You can use the AUDITSTORAGE server option to specify that storage is not to be calculated as part of a license audit.

You can use the information from this query to determine if and where client node storage utilization must be balanced. This information can also assist you with billing clients for storage usage.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

node_name
: Specifies a list of nodes for which to display server storage use information. Specify more than one node by separating the node names with commas, with no intervening spaces. You can use wildcard characters to specify names. The default (*) is to query all client nodes. Use the DOMAIN parameter to limit this list by policy domain. This parameter is optional.

DOmain
: Specifies a list of policy domains to restrict which nodes are displayed. Nodes belonging to the specified policy domains are displayed. Specify more than one policy domain by separating the policy domain names with commas, with no intervening spaces. You can use wildcard characters to specify names. This parameter is optional.

POoltype
: Specifies the type of storage pool to display. This parameter is optional. The default is ANY. Possible values are:

  ANY
  : Specifies both primary and copy storage pools. The value that is presented is the total for the two pools.

  PRimary
  : Specifies primary storage pools only.

  COpy

Specifies copy storage pools only.

Example: Display storage usage

Display combined storage use in primary and copy storage pools. Issue the command:

```
query auditoccupancy
```

```
License information as of last audit on 05/22/1996 14:49:51.

       Node Name          Backup    Archive  Space-Managed    Total
                         Storage    Storage  Storage Used   Storage
                       Used (MB)  Used (MB)       (MB)     Used (MB)
--------------------   ---------  ---------- ------------   ---------
CLIENT                       245         20          0            265
SMITH                        245         20          0            265
SMITHERS                     245         20          0            265
JOHNSON                      300         15          0            320
JOE                          245         20          0            265
TOM                          300         15          0            320
LARRY                        245         20          0            265
```

See Field descriptions for field descriptions.

Field descriptions

Node Name
: Specifies the name of the client node.

Backup Storage Used (MB)
: Specifies the total backup storage use for the node. For this value, one MB = 1048576 bytes.

Archive Storage Used (MB)
: Specifies the total archive storage use for the node. For this value, one MB = 1048576 bytes.

Space-Managed Storage Used (MB)
: Specifies the amount of server storage that is used to store files that are migrated from the client node by an IBM Spectrum Protect™ for Space Management client. For this value, one MB = 1048576 bytes.

Total Storage Used (MB)
: Specifies the total storage use for the node. For this value, one MB = 1048576 bytes.

Related commands

Table 1. Commands related to QUERY AUDITOCCUPANCY

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.
QUERY LICENSE	Displays information about licenses and audits.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER LICENSE	Registers a license with the IBM Spectrum Protect server.
SET LICENSEAUDITPERIOD	Specifies the number of days between automatic license audits.

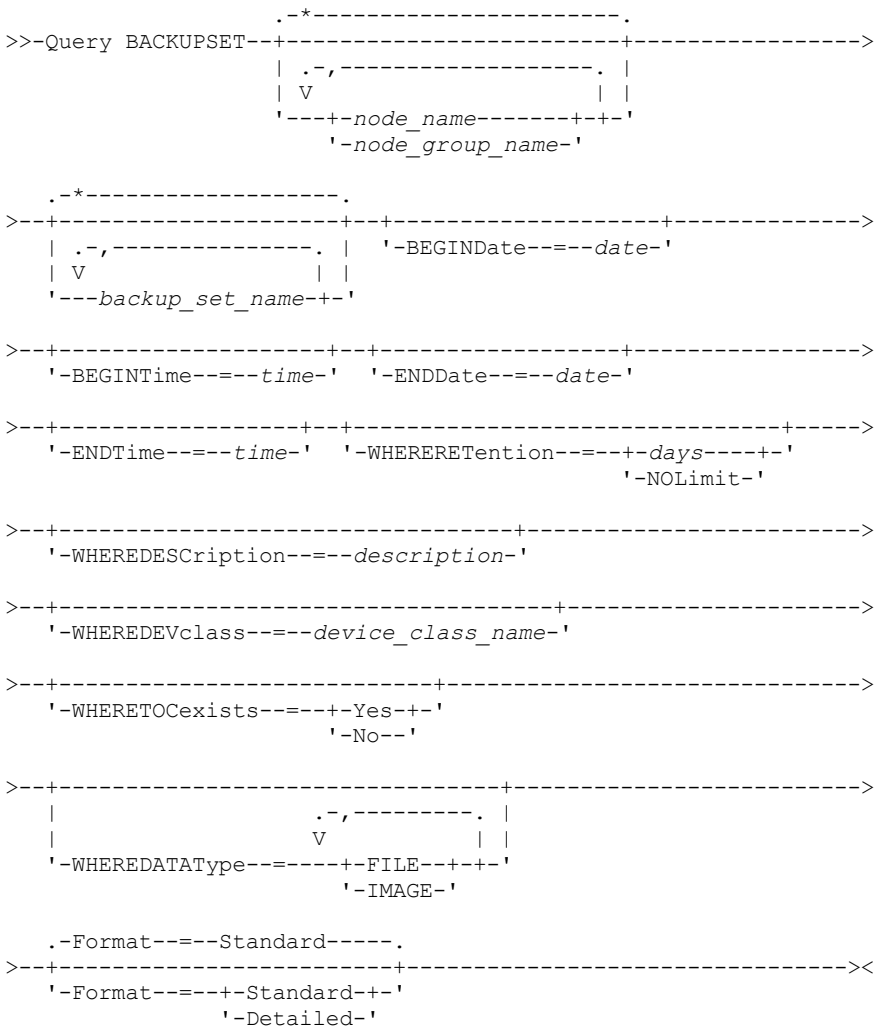
QUERY BACKUPSET (Query a backup set)

Use this command to display information about one or more backup sets.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

node_name or node_group_name
: Specifies the name of the client node and node groups whose data is contained in the backup set to be displayed. To specify multiple node names and node group names, separate the names with commas and no intervening spaces. You can use wildcard characters with node names but not with node group names.

backup_set_name
: Specifies the name of the backup set whose information is to be displayed. The backup set name you specify can contain wildcard characters. You can specify more than one backup set name by separating the names with commas and no intervening spaces.

BEGINDate
: Specifies the beginning date of the range in which the point-in-time date of the backup set to be displayed must fall. This parameter is optional. You can use this parameter with the BEGINTIME parameter to specify a range for the date and time. If you specify a begin date without a begin time, the time will be at 12:00 a.m. (midnight) on the date you specify.
You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified.	TODAY +3 *or* +3.
TODAY-days *or* -days	The current date minus days specified.	TODAY -3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM

Value	Description	Example
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time of the range in which the point-in-time date of the backup set to be displayed must fall. This parameter is optional. You can use this parameter with the BEGINDATE parameter to specify a range for the date and time. If you specify a begin time without a begin date, the date will be the current date at the time you specify.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes specified	NOW+02:00 *or* +02:00.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes specified	NOW-02:00 *or* –02:00.

ENDDate

Specifies the ending date of the range in which the point-in-time date of the backup set to be displayed must fall. This parameter is optional. You can use this parameter with the ENDTIME parameter to specify an ending date and time. If you specify an end date without an end time, the time will be at 11:59:59 p.m. on the specified end date.

You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 *or* +3.
TODAY-days *or* -days	The current date minus days specified.	TODAY -3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time of the range in which the point-in-time date of the backup set to be displayed must fall. This parameter is optional. You can use this parameter with the ENDDATE parameter to specify a date and time. If you specify an end time without an end date, the date will be the current date at the time you specify.

You can specify the time by using one of the following values:

Value	Description	Example

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes specified	NOW+02:00 *or* +02:00.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes specified	NOW-02:00 *or* –02:00.

WHERERETention
: Specifies the retention value, specified in days, that must be associated with the backup sets to be displayed. You can specify an integer from 0 to 30000. The values are:

  days
  : Specifies that backup sets that are retained this number of days are displayed.

  NOLimit
  : Specifies that backup sets that are retained indefinitely are displayed.

WHEREDESCription
: Specifies the description that must be associated with the backup set to be displayed. The description you specify can contain wildcard characters. This parameter is optional. Enclose the description in quotation marks if it contains any blank characters.

WHEREDEVclass
: Specifies the name of the device class that must be associated with the backup set to be displayed. You can use wildcard characters to specify a device class name. This parameter is optional.

WHERETOCexists
: Specifies whether a backup set must have a table of contents in order to be displayed. This parameter is optional. The default is to display all backup sets whether or not they have a table of contents.

WHEREDATAType
: Specifies the data type of a backup set to be displayed. This parameter is optional. The default is to display all types of backup sets. To specify multiple data types, separate data types with commas and no intervening spaces.

  FILE
  : Specifies that a file level backup set is to be displayed. File level backup sets contain files and directories backed up by the backup-archive client.

  IMAGE
  : Specifies that an image backup set is to be displayed. Image backup sets contain images created by the backup-archive client BACKUP IMAGE command.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the specified backup sets.

  Detailed
  : Specifies that complete information is displayed for the specified backup sets.

Example: Query a backup set

Display information for backup sets whose names begin with PERS_DATA. The backup sets belong to the node JANE and are assigned to the DVLMENT device class.

```
query backupset jane pers_data*

                 Node Name: JANE
           Backup Set Name: PERS_DATA.3089
                 Data Type: File
                 Date/Time: 03/17/2007 16:17:47
          Retention Period: 60
        Device Class Name: DVLMENT
              Description: backupset created from /srvr
Has Table of Contents (TOC)?: Yes
```

Field descriptions

Node Name
: Specifies the name of the client node whose data is contained in the backup set.

Backup Set Name
: Specifies the name of the backup set.

Data Type
: Displays the data type of the backup sets. Possible types are file, image, and application.

Date/Time
: Specifies the date and time (PITDate and PITTime) of the GENERATE BACKUPSET command. The PITDate and PITTime specify that files that were active on the specified date and time and that are still stored on the IBM Spectrum Protect™ server are to be included in the backup set, even if they are inactive at the time you issue the GENERATE BACKUPSET command. The default is the date on which the GENERATE BACKUPSET command is run.

Retention Period
: Specifies the number of days that the backup set is retained on the server.

Device Class Name
: Specifies the name of the device class for which the volumes containing the backup set is assigned.

Description
: Specifies the description associated with the backup set.

Has Table of Contents (TOC)?
: Specifies whether the backup set has a table of contents.

Related commands

Table 1. Commands related to QUERY BACKUPSET

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

QUERY BACKUPSETCONTENTS (Query contents of a backup set)

Use this command to display information about the files and directories contained in a backup set for a client node.

Remember: Processing this command can use considerable network resources and mount points.

Privilege class

To issue this command, you must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax

```
>>-Query BACKUPSETCONTENTS--node_name--backup_set_name---------->

   .-DATAType--=--FILE------.
>--+------------------------+--------------------------------><
   '-DATAType--=--+-FILE--+-'
```

```
'-IMAGE-'
```

Parameters

node_name (Required)
: Specifies the name of the client node whose data is contained in the backup set to display. The name you specify cannot contain wildcard characters nor can it be a list of node names separated by commas.

backup_set_name (Required)
: Specifies the name of the backup set to display. The name that you specify cannot contain wildcard characters nor can it be a list of node names that are separated by commas.

DATAType
: Specifies that the backup set containing the specified types of data is to be queried. This parameter is optional. The default is that a file level backup set is to be queried. Possible values are:

  FILE
  : Specifies that a file level backup set is to be queried. File level backup sets contain files and directories backed up by the backup-archive client.

  IMAGE
  : Specifies that an image backup set is to be queried. Image backup sets contain images created by the backup-archive client BACKUP IMAGE command.

Example: Query contents of a backup set for a specific node

Display the contents from backup set named PERS_DATA.3099 belonging to client node JANE. Issue the command:

```
query backupsetcontents jane pers_data.3099

Node Name                Filespace  Client's Name for File
                         Name
------------------------ ---------- ------------------------
JANE                     /srvr      /deblock
JANE                     /srvr      /deblock.c
JANE                     /srvr      /dsmerror.log
JANE                     /srvr      /dsmxxxxx.log
JANE                     ...        ......
```

Field descriptions

Node Name
: Specifies the name of the client node whose data is contained in the backup set.

Filespace Name
: Specifies the name of the file space to which the specified file belongs.

  File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

  If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

Client's Name for File
: Specifies the name of the file.

  File space names and file names that can be in a different code page or locale than the server do not display correctly in the Operations Center or the administrative command-line interface. The data itself is backed up and can be restored properly, but the file space or file name may display with a combination of invalid characters or blank spaces.

  If the file space name is Unicode enabled, the name is converted to the server's code page for display. The results of the conversion for characters not supported by the current code page depends on the operating system. For names that IBM Spectrum Protect™ is able to partially convert, you may see question marks (??), blanks, unprintable characters, or "...".

These characters indicate to the administrator that files do exist. If the conversion is not successful, the name is displayed as "...". Conversion can fail if the string includes characters that are not available in the server code page, or if the server has a problem accessing system conversion routines.

A file name that is displayed as "....." indicates that both the file path and file name were not successfully converted. An example of the path and name could be:

```
my\dir\...
```

Related commands

Table 1. Commands related to QUERY BACKUPSETCONTENTS

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
DELETE BACKUPSET	Deletes a backup set.
QUERY BACKUPSET	Displays backup sets.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.

AIX | Linux | Windows

QUERY CLEANUP (Query the cleanup that is required in a source storage pool)

Use this command to display information about damaged files that are identified during a storage pool conversion process.

When you issue the CONVERT STGPOOL command to convert a FILE device class, a tape device class, or a virtual tape library (VTL) to a directory-container storage pool, some files in the source storage pool might not convert because of damaged data. To display damaged data that is identified during the conversion process, issue the QUERY CLEANUP command on a source storage pool.

To recover an undamaged version of the data from a copy or active-data storage pool, issue the RESTORE STGPOOL command. To recover an undamaged version of the data from a target replication server issue the REPLICATE NODE command and specify the RECOVERDAMAGED=YES parameter.

Privilege class

To issue this command, you must have restricted storage privilege.

Syntax

```
>>-Query CLeanup--pool_name-------------------------------------><
```

Parameters

pool_name(Required)
Specifies the storage pool to query.

Example: Display damaged files that are identified by a storage pool conversion process

Display damaged files in a storage pool that is named POOL1. See Field descriptions for field descriptions.

```
query cleanup pool1

             File Name: \RTC\BDAT\GIGFILES\BF1.GB
                 State: Active
           Stored Size: 1 GB
```

```
     Filespace Name: \\ibm838-r90gf0gx\c$
               Type: Backup
        Client Name: CAKINProtection
    Protection Date: 03/25/2016 16:47:57
```

Field descriptions

File Name
: The name of the damaged file.

State
: The state of the data in the inventory. The following states are possible:

  Active
  : The version of the file in the inventory is active. You can have only one active version of the file in the inventory.

  Inactive
  : The version of the file in the inventory is inactive. You can have multiple inactive versions of the file in the inventory.

Stored Size
: The size of the data, in megabytes (MB) or gigabytes (GB), that is stored in the storage pool.

Filespace Name
: The name of the file space where the file is assigned.

Type
: The type of operation that was used to store the file. The following types are possible:

  Backup
  : Files that are backed up.

  Archive
  : Files that are archived.

  SpaceMg
  : Files that are migrated from an IBM Spectrum Protect™ for Space Management client.

Client Name
: The name of the client that owns the file.

Protection Date
: The time and date that the file was backed up, archived, or migrated by an IBM Spectrum Protect for Space Management client.

Related commands

Table 1. Commands related to QUERY CLEANUP

Command	Description
CONVERT STGPOOL	Convert a storage pool to a directory-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
QUERY CONVERSION	Query conversion status of a storage pool.
REMOVE DAMAGED	Removes damaged data from a source storage pool.
REPAIR STGPOOL	Repairs a directory-container storage pool.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.

QUERY CLOPTSET (Query a client option set)

Use this command to query a client option set.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*---------------.
>>-Query CLOptset--+-----------------+-------------------------->
                    '-option_set_name-'

>--+-----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

option_set_name
: Specifies the name of the client option set to be queried. You can use wildcard characters to specify this name. This parameter is optional. The default is option set names.

DESCription
: Specifies the description used on the DEFINE or UPDATE CLOPTSET commands to be used as a filter. If the description contains spaces, enclose it in quotation marks. This parameter is optional.

Example: Query a client option set

From a managed server, query a client option set named ENG. Issue the following command:

```
query cloptset eng
```

```
                     Optionset:  ENG
                   Description:
Last Update by (administrator): $$CONFIG_MANAGER$$
              Managing profile:
            Replica Option Set: Yes

                        Option: SCROLLINES
                Sequence number: 0
  Use Option Set Value (FORCE): No
                  Option Value: 40

                        Option: SCROLLPROMPT
                Sequence number: 0
  Use Option Set Value (FORCE): No
                  Option Value: yes
```

Field descriptions

Optionset
: Specifies the name of the option set.

Description
: Specifies the description of the client option set.

Last Update by (administrator)
: Specifies the name of the administrator that most recently updated the option set. If this field contains $$CONFIG_MANAGER$$, the client option set is associated with a profile that is managed by the configuration manager.

Managing profile
: Specifies the profile to which the managed server subscribed to get the definition of the client option set.

Replica Option Set
: Specifies the replica option set is replicated by the source replication server.

Option
: Specifies the name of the option.

Sequence number
: Specifies the sequence number of the option.

Use Option Set Value (FORCE)
: Specifies whether the server option setting overrides the option setting for the client. NO indicates that the server option setting does not override the client option. YES indicates that the server option setting overrides the client option setting. This option is set with the FORCE parameter on the DEFINE CLIENTOPT command.

Option Value

Specifies the value of the option.

Related commands

Table 1. Commands related to QUERY CLOPTSET

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.
UPDATE CLOPTSET	Updates the description of a client option set.
DEFINE PROFASSOCIATION	Associates objects with a profile.

QUERY COLLOCGROUP (Query a collocation group)

Use this command to display the collocation groups defined on the server.

Privilege class

Any administrator can issue this command.

Syntax

```
                      .-*----------.
>>-Query COLLOCGroup--+------------+---------------------------->
                      '-group_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

group_name
: Specifies the name of the collocation group to display. To specify multiple names, use a wildcard character. This parameter is optional. The default is to display all collocation groups.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed. To display the members of the collocation group, you must specify FORMAT=DETAILED.

Display defined collocation groups

Display the collocation groups defined on the server. Issue the following command:

```
query collocgroup

Collocation Group Name         Collocation Group Description
-------------------------     ------------------------------
```

```
DEPT_ED                         Education department
GROUP1                          Low cap client nodes.
```

See Field descriptions for field descriptions.

Display detailed information for collocation groups

Display complete information about all collocation groups and determine which client nodes belong to which collocation groups. Issue the following command:

```
query collocgroup format=detailed

        Collocation Group Name: DEPT_ED
 Collocation Group Description: Education department
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2013 10:59:03
   Collocation Group Member(s): EDU_1 EDU_7
           Filespace Member(s):

        Collocation Group Name: GROUP1
 Collocation Group Description: Low cap client nodes.
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2013 10:59:16
   Collocation Group Member(s): CHESTER
           Filespace Member(s): alpha

        Collocation Group Name: GROUP1
 Collocation Group Description: Low cap client nodes.
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2013 10:59:16
   Collocation Group Member(s): CHESTER
           Filespace Member(s): beta

        Collocation Group Name: GROUP1
 Collocation Group Description: Low cap client nodes.
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2013 10:59:16
   Collocation Group Member(s): CHESTER
           Filespace Member(s): gamma
```

See Field descriptions for field descriptions.

Field descriptions

Collocation Group Name
: The name of the collocation group.

Collocation Group Description
: The description for the collocation group.

Last Update by (administrator)
: The name of the administrator that defined or most recently updated the collocation group.

Last Update Date/Time
: The date and time that an administrator defined or most recently updated the collocation group.

Collocation Group Member(s)
: The members of the collocation group.

Filespace Member(s)
: The file space or file spaces that are members of the collocation group. If there is more than one file space, each file space is displayed in a separate entry.

Related commands

Table 1. Commands related to QUERY COLLOCGROUP

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

AIX Linux Windows

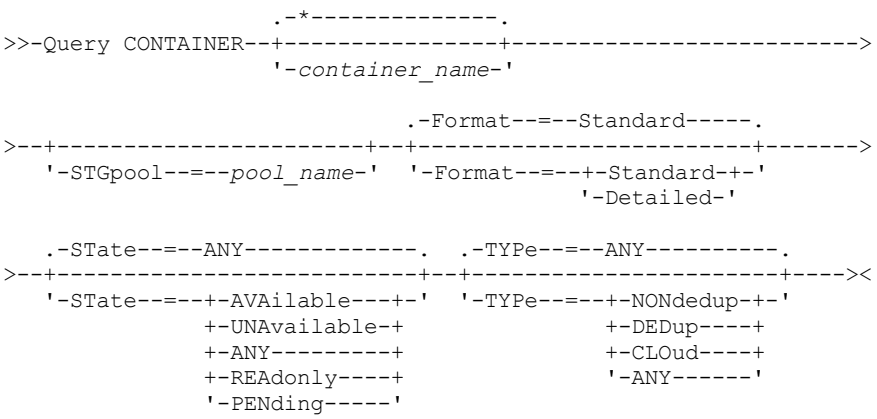
QUERY CONTAINER (Query a container)

Use this command to display information about one or more containers.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

container_name
: Specifies the name of the container. Specify one of the following values:

  *
  : Specifies that an asterisk (*) represents a wildcard character. Use wildcard characters such as an asterisk to match any characters. Alternatively, you can use a question mark (?) or a percent sign (%) to match exactly one character. If you specify an asterisk, all container names are displayed. This value is the default.

  container_name
  : Specifies the name of the container. The maximum length of the file name is 1024.

STGpool
Specifies the name of the directory-container storage pool. This parameter is optional. The maximum length of the storage pool name is 30.

Format
Specifies the level of detail of the query results. This parameter is optional. Specify one of the following values:

Standard
Specifies that a summary of the information is displayed. This value is the default.

Detailed
Specifies that detailed information is displayed.

STate
Specifies the state of the container that is queried. This parameter is optional. Specify one of the following values:

AVAilable
Specifies that only containers that are available are displayed.

UNAvailable
Specifies that only containers that are not available are displayed. For example, a container might be unavailable if the header is corrupted or if the container cannot be opened.

ANY
Specifies that containers in any state are displayed. This value is the default.

REAdonly
Specifies that only containers in a read-only state are displayed. Data in the container can be read but data cannot be written to the container.

PENding
Specifies that only containers in a pending state are displayed.

TYPe
Specifies the type of container that is queried. This parameter is optional. Specify one of the following values:

NONdedup
Displays containers that contain data that is not deduplicated. This type of data includes metadata, encrypted data, and data that is too small for data deduplication.

DEDup
Displays containers that contain deduplicated data.

CLOud
Displays containers that are stored in a cloud storage pool.

ANY
Displays any type of container. This value is the default.

AIX | Linux

Example: Display information about a container

See Field descriptions for field descriptions.

```
query container /Containers/09/0000000000000943.ncf
```

```
Container                              Storage       Container     State
                                       Pool Name     Type
-----------------------------------  ------------- ------------  ---------
/Containers/09/0000000000000943.ncf   STGPOOL1      Non Dedup     Available
```

Windows

Example: Display information about a container

See Field descriptions for field descriptions.

```
query container C:\abc\00\0000000000000005.ncf
```

```
Container                          Storage      Container   State
                                   Pool Name    Type
-------------------------------    -----------  ----------  ---------
C:\abc\00\0000000000000005.ncf     STGPOOL1     Non Dedup   Available
```

AIX | Linux

Example: Display detailed information about a container

Display detailed information about containers that contain deduplicated data in storage pool STGPOOL1:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
                         Container: /abc/00/0000000000000001.dcf
                 Storage Pool Name: STGPOOL1
                    Container Type: Dedup
                             State: Available
                 Maximum size (MB): 40,960
                   Free Space (MB): 39,700
          Approx. Date Last Written: 11/10/2014 15:17:09
            Approx. Date Last Audit:
                        Cloud Type:
                         Cloud URL:
             Cloud Object Size (MB):
                Space Utilized (MB):
                  Data Extent Count:
```

Windows

Example: Display detailed information about a container

Display detailed information about containers that contain deduplicated data in storage pool STGPOOL1:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
                         Container: C:\abc\00\0000000000000001.dcf
                 Storage Pool Name: STGPOOL1
                    Container Type: Dedup
                             State: Available
                 Maximum size (MB): 40,960
                   Free Space (MB): 39,700
          Approx. Date Last Written: 11/10/2014 15:17:09
            Approx. Date Last Audit:
                        Cloud Type:
                         Cloud URL:
             Cloud Object Size (MB):
                Space Utilized (MB):
                  Data Extent Count:
```

Example: Display detailed information about containers that are stored in a cloud storage pool

Display detailed information about containers that are stored in the cloud storage pool CLOUDPOOL:

```
query container stgpool=CLOUDPOOL format=detail
```

```
                          Container: 7-64a1261000c811e58e8f005056c00008
                  Storage Pool Name: CLOUDPOOL
                     Container Type: Cloud
                              State:
                    Free Space (MB):
                   Maximum Size (MB):
          Approx. Date Last Written: 05/22/2015 14:36:57
            Approx. Date Last Audit:
                         Cloud Type: SWIFT
                          Cloud URL: http://cloudurl:5000/v2.0
             Cloud Object Size (MB):
                Space Utilized (MB): 27
                  Data Extent Count: 95
```

Field descriptions

Container
: The name of the container.

Storage Pool Name
: The name of the storage pool.

Container Type
: The type of container.

State
The state of the data in the container. The field can contain one of the following values:

Available
The container is available for use.
Unavailable
The container cannot be opened or validated.
Tip: Issue the AUDIT CONTAINER command to validate the contents of the container.
Read only
The container can be read but data cannot be written to the container.
Pending
The container is pending deletion. When the value that is specified for the REUSEDELAY parameter expires on the DEFINE STGPOOL or UPDATE STGPOOL command, the container is deleted.

In general, this field does not apply to containers that are stored in cloud-container storage pools. However, if a container in a cloud-container storage pool is moved by using the MOVE CONTAINER command with the DEFRAG=YES setting, the container is in pending state until it is deleted.

Maximum Size (MB)
The maximum size of the container, in megabytes.

This field does not apply to containers that are stored in cloud storage pools.

Free Space (MB)
The total amount of free space that is available in the container, in megabytes.

This field does not apply to containers that are stored in cloud storage pools.

Approx. Date Last Written
The approximate date and time that data was written to the container.
Approx. Date Last Audit
The approximate date and time that data was audited in the container.
Cloud Type
If the container is stored in a cloud storage pool, the type of cloud platform.
Cloud URL
If the container is stored in a cloud storage pool, the URL for accessing the on-premises private cloud or off-premises public cloud.
Cloud Object Size (MB)
The size of the cloud object, in megabytes, if the container is represented by a single object in the cloud-container storage pool.
Space Utilized (MB)
If the container is stored in a cloud storage pool, the amount of space that is used by the container in the on-premises private cloud or off-premises public cloud.
Data Extent Count
If the container is stored in a cloud-container storage pool, the number of data extents that are managed by the on-premises private cloud or off-premises public cloud for the container.

Table 1. Commands related to QUERY CONTAINER

Command	Description
AUDIT CONTAINER	Audit a directory-container storage pool.
MOVE CONTAINER	Moves the contents of a storage pool container to another container.
QUERY DAMAGED	Displays information about damaged files.

QUERY CONTENT (Query the contents of a storage pool volume)

Use this command to display information about files in a storage pool volume, and the names of client files that link to a deduplicated group of files.

You can use this command to identify files that the server found to be damaged and files that were backed up to a copy storage pool or copied to an active-data pool. This command is useful when a volume is damaged or before you:

- Request the server to fix inconsistencies between a volume and the database
- Move files from one volume to another volume
- Delete a volume from a storage pool

Because this command can take a long time to run and the results can be large, consider using the COUNT parameter to limit the number of files displayed.

Note: Files that are cached in a disk volume and that are marked as damaged are not included in the results.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query CONtent--volume_name--+--------------------+----------->
                               '-NODE--=--node_name-'

>--+-------------------------------+--+------------------+------>
   '-FIlespace--=--file_space_name-'  '-COUnt--=--number-'

   .-Type--=--ANY--------------.  .-Format--=--Standard-----.
>--+---------------------------+--+-------------------------+--->
   '-Type--=--+-ANY-----------+-'  '-Format--=--+-Standard-+-'
              +-Backup-------+                  '-Detailed-'
              +-Archive------+
              '-SPacemanaged-'

                                    (1)
   .-DAmaged--=--ANY-----.  .-COPied------=--ANY-.
>--+---------------------+--+--------------------+-------------->
   '-DAmaged--=--+-ANY-+-'  '-COPied--=--+-ANY-+-'
                 +-Yes-+                 +-Yes-+
                 '-No--'                 '-No--'

   .-NAMEType--=--SERVER------.
>--+--------------------------+--------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+------------------------------->
   '-CODEType--=--+-UNIcode----+-'
                  +-NONUNIcode-+
                  '-BOTH-------'

   .-FOLLOWLinks--=--No------------.
>--+-------------------------------+---------------------------><
   '-FOLLOWLinks--=--+-No--------+-'
                     +-Yes-------+
                     '-JUSTLinks-'
```

Notes:

1. Use this parameter only for volumes in primary storage pools.

Parameters

volume_name (Required)
: Specifies the volume to be queried.

NODE
: Specifies the backup-archive client or the IBM Spectrum Protect™ for Space Management associated with the file space to query. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a name, all backup-archive and IBM Spectrum Protect for Space Management clients are included.

FIlespace

Specifies the file space to query. This parameter is optional. You can use wildcard characters to specify this name. File space names are case-sensitive. If you do not specify a file space name, all file spaces are included.

For a server that has clients with Unicode support, you might need to have the server convert the file space name that you enter. For example, you might need to have the server convert the name that you enter from the server's code page to Unicode. See the NAMETYPE parameter for details. If you do not specify a file space name or specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or non-Unicode file spaces.

COUnt
: Specifies the number of files to be displayed. This parameter is optional. You can specify either a positive integer or a negative integer. If you specify a positive integer, *n*, the first `n` files are displayed. If you specify a negative integer, *-n*, the last `n` files are displayed in `reverse` order. You cannot specify COUNT=0. If you do not specify a value for this parameter, all files are displayed.

Type
: Specifies the types of files to query. This parameter is optional. The default value is ANY. If the volume that is being queried is assigned to an active-data pool, the only valid values are ANY and BACKUP. Possible values are:

  ANY
  : Specifies that all types of files in the storage pool volume are queried; backup versions of files, archived copies of files, and files that are migrated by IBM Spectrum Protect for Space Management clients from client nodes.

  Backup
  : Specifies that only backup files are queried.

  Archive
  : Specifies that only archive files are queried. This value is not valid for active-data pools.

  SPacemanaged
  : Specifies that only space-managed files (files that were migrated by an IBM Spectrum Protect for Space Management client) are queried. This value is not valid for active-data pools.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed. Unicode names are converted to the server code page.

  Detailed
  : Specifies that complete information is displayed. Unicode names are displayed in hexadecimal.

DAmaged
: Specifies criteria to restrict the query output based on whether files are marked as damaged. For purposes of this criteria, the server examines only physical files (a file that might be a single logical file or an aggregate that consists of logical files). This parameter is optional. The default value is ANY. Possible values are:

  ANY
  : Specifies that files are displayed regardless of whether the server found the files to be damaged.

  Yes
  : Specifies that only files that are marked as damaged are displayed. These are files in which the server found errors when a user attempted to restore, retrieve, or recall the file, or when an AUDIT VOLUME command was run.

  No
  : Specifies that only files not known to be damaged are displayed.

COPied
: Specifies criteria to restrict the query output based on whether files were backed up to a copy storage pool. Whether files are stored in an active-data pool does not affect the output. This parameter is optional. The default value is ANY. Possible values are:

  ANY
  : Specifies that files are displayed regardless of whether the files are backed up to a copy storage pool. Primary and cached file copies are displayed.

  Yes
  : Specifies that the files displayed are only those for which at least one usable backup copy exists in a copy storage pool. A file is not displayed if its copy in the copy storage pool is known to have errors. Cached file copies are not displayed because these files are never restored.

Use COPIED=YES to identify primary files that can be restored using the RESTORE VOLUME or RESTORE STGPOOL command.

No
: Specifies that the files displayed are only those for which no usable backup copies exist in a copy storage pool. Cached file copies are not displayed because these files are never restored.

  Use COPIED=NO to identify primary files that cannot be restored using the RESTORE VOLUME or RESTORE STGPOOL command.

NAMEType
: Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with Unicode support. A backup-archive client with Unicode support is currently available only for Windows, Macintosh OS 9, Macintosh OS X, and NetWare. Use this parameter only when you specify a partly or fully qualified file space name.

  The default value is SERVER. Possible values are:

  SERVER
  : The server uses the server's code page to interpret the file space names.

  UNIcode
  : The server converts the file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the names and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has a problem accessing system conversion routines.

  FSID
  : The server interprets the file space names as their file space IDs (FSIDs).

CODEType
: Specify how you want the server to interpret the file space names that you enter. Use this parameter only when you enter a single wildcard character for the file space name.

  The default value is BOTH, which means that the file spaces are included regardless of code page type. Possible values are:

  UNIcode
  : Include file spaces that are only in Unicode.

  NONUNIcode
  : Include file spaces that are not only in Unicode.

  BOTH
  : Include file spaces regardless of code page type.

FOLLOWLinks
: Specifies whether to display only the files that are stored on the volume or only files that are linked to the volume. You can also display both stored files and linked files. The default is NO. Possible values are:

  No
  : Display only the files that are stored in the volume. Do not display files that have links to the volume.

  Yes
  : Display all files, including files that are stored on the volume and any files that have links to the volume.

  JUSTLinks
  : Display only the files that have links to the volume. Do not display files that are stored on the volume.

Example: Display the contents of a volume for a specific client node

Query the contents of a volume and limit the results to files backed up from the PEGASUS client node.

AIX Linux For the volume /tsmstg/diskvol1.dsm, issue the command:

```
query content /tsmstg/diskvol1.dsm node=pegasus
 type=backup
```

Windows For the volume f:\tsmstg\diskvol1.dsm, issue the command:

```
query content f:\tsmstg\diskvol1.dsm node=pegasus
 type=backup
```

Results of the command include all logical files that make up any aggregate that is on the volume, even if the aggregate is stored on more than this volume. For aggregates, the query does not determine which logical files are actually stored on the volume for which the query is performed.

```
Node Name     Type  Filespace     FSID  Client's Name for File
                    Name
-----------   ----  ----------    ----  ----------------------
PEGASUS       Bkup  \\pegasus\e$    1   \UNI_TEST\ SM01.DAT
PEGASUS       Bkup  \\pegasus\e$    1   \UNI_TEST\ SM02.DAT
```

See Field descriptions for field descriptions.

Example: Display detailed information for a tape volume

Query the contents of the tape volume named WPD001. Display only files that are backed up by the node MARK, and files that are either stored on the volume or linked to the volume. Display only the first four files on the volume.

```
query content wpd001 node=mark count=4 type=backup followlinks=yes
 format=detailed

                         Node Name: MARK
                              Type: Bkup
                   Filespace Name: \\mark\e$
        Hexadecimal Filespace Name:
                              FSID: 1
            Client's Name for File: \UNI_TEST\ SM01.DAT
Hexadecimal Client's Name for File:
                      Aggregated?: 1/3
                      Stored Size: 2,746
                   Segment Number:
                     Cached Copy?: No
                           Linked: No
                  Fragment Number:

                         Node Name: MARK
                              Type: Bkup
                   Filespace Name: \\mark\e$
        Hexadecimal Filespace Name:
                              FSID: 1
            Client's Name for File: \UNI_TEST\ SM02.DAT
Hexadecimal Client's Name for File:
                      Aggregated?: 2/3
                      Stored Size: 2,746
                   Segment Number:
                     Cached Copy?: No
                           Linked: No
                  Fragment Number: 2

                         Node Name: MARK
                              Type: Bkup
                   Filespace Name: \\mark\e$
        Hexadecimal Filespace Name:
                              FSID: 1
            Client's Name for File: \UNI_TEST\ SM03.DAT
Hexadecimal Client's Name for File:
                      Aggregated?: 3/3
                      Stored Size: 2,746
                   Segment Number:
                     Cached Copy?: No
                           Linked: No
                  Fragment Number: 3
```

See Field descriptions for field descriptions.

Field descriptions

Node Name
: The node to which the file belongs.

Type

The type of file: archive (Arch), backup (Bkup), or space-managed (SpMg) by an IBM Spectrum Protect for Space Management client.

Filespace Name
The file space to which the file belongs.

File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

Hexadecimal Filespace Name
The file space to which the file belongs. If the file space name is in Unicode, the name is displayed in hexadecimal format.

FSID
The file space ID (FSID) for the file space. The server assigns a unique FSID when a file space is first stored on the server.

Client's Name for File
The client's name for the file.

File space names and file names that can be in a different code page or locale than the server do not display correctly in the Operations Center or the administrative command-line interface. The data itself is backed up and can be restored properly, but the file space or file name might display with a combination of invalid characters or blank spaces. The results of the conversion for characters that are not supported by the current code page depends on the operating system. For names that IBM Spectrum Protect is able to partially convert, you might see question marks (??), blanks, unprintable characters, or "...". These characters indicate to the administrator that files do exist.

Hexadecimal Client's Name for File
The client's name for the file that is displayed in hexadecimal format.

Aggregated?
Whether the file is a logical file that is stored as part of an aggregate. If the file is part of an aggregate, the sequence of this file within the aggregate and the total number of logical files in the aggregate are displayed. Results of the command include all logical files that make up any aggregate that is on the volume, even if the aggregate is stored on more than this volume. The query does not determine which logical files are actually stored on the volume for which the query is performed.

If the file is not part of an aggregate, the field displays "no".

Stored Size
The size of the physical file, in bytes. If the file is a logical file that is stored as part of an aggregate, this value indicates the size of the entire aggregate.

Segment Number
For volumes in sequential-access storage pools, specifies whether the physical file (either a single logical file or an aggregate of logical files) is stored across multiple volumes. For example, if the logical file is stored in an aggregate that spans two volumes, the segment number indicates `1/2` (the first part of the physical file is stored on the volume) or `2/2` (the second part of the physical file is stored on the volume). If the segment number is `1/1`, the physical file is completely stored on the volume. For volumes in random-access storage pools, no value is displayed for this field.

Cached Copy?
Whether the physical file is a cached copy of a file migrated to the next storage pool. If the file is part of an aggregate, this value pertains to the aggregate.

Linked
Indicates whether the file is stored on the volume or whether the file is linked to the volume.

Fragment Number
Specifies the fragment number. If the fragment number is blank, it is either the first fragment or not a fragment.

Related commands

Table 1. Commands related to QUERY CONTENT

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.

Command	Description
COPY ACTIVEDATA	Copies active backup data.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE VOLUME	Deletes a volume from a storage pool.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
UPDATE VOLUME	Updates the attributes of storage pool volumes.

AIX Linux Windows

QUERY CONVERSION (Query conversion status of a storage pool)

Use this command to display information about a conversion operation. You can convert a primary storage pool that uses a FILE type device class or a virtual tape library (VTL) to a directory-container storage pool.

Privilege class

To issue this command, you must have restricted storage privilege.

Syntax

```
>>-Query CONVERSion--+-----------+------------------------------>
                     '-pool_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

pool_name
: Specifies the source storage pool to query. This parameter is optional. If you do not specify a value for this parameter, information is displayed for all storage pools.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Specify one of the following values:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display conversion information for all storage pools

Display conversion information for all storage pools. See Field descriptions for field descriptions.

```
query conversion

Source Storage  Target Storage  Starting   Total       Last
    Pool              Pool      Amount     Converted   Converted
-------------  ---------------  ---------  ----------  ----------
FILEPOOL         CTR             3 GB       3 GB        3 GB
FPOOL            CTR             333 MB     333 MB      267 MB
```

Example: Display detailed about storage pool conversion

Display detailed information about storage pool conversion. See Field descriptions for field descriptions.

```
query conversion format=detailed

    Source Storage Pool: FILEPOOL
    Target Storage Pool: CTR
      Maximum Processes: 4
               Duration: 60 minutes
      Starting Amount: 333 MB
      Total Converted: 333 MB
       Last Converted: 333 MB
      Start Date/Time: 03/24/2016 13:22:32
```

Field descriptions

Source Storage Pool
: The name of the storage pool that is being converted.

Target Storage Pool
: The name of the destination storage pool, where the converted data will be stored.

Maximum Processes
: Specifies the maximum number of conversion processes.

Duration
: Specifies the length of time, in minutes, for conversion.

Starting Amount
: The starting amount of data to convert, in megabytes (MB), gigabytes (GB), or terabytes (TB).

Total Converted
: The total amount of data that is converted, in megabytes (MB), gigabytes (GB), or terabytes (TB).

Last Converted
: The amount of data, in megabytes (MB), gigabytes (GB), or terabytes (TB), that is converted during this conversion process.

Start Date/Time
: The time and date that the CONVERT STGPOOL command was first issued for the storage pool.

Related commands

Table 1. Commands related to QUERY CONVERSION

Command	Description
CONVERT STGPOOL	Convert a storage pool to a directory-container storage pool.
QUERY CLEANUP	Query the cleanup status of a source storage pool.

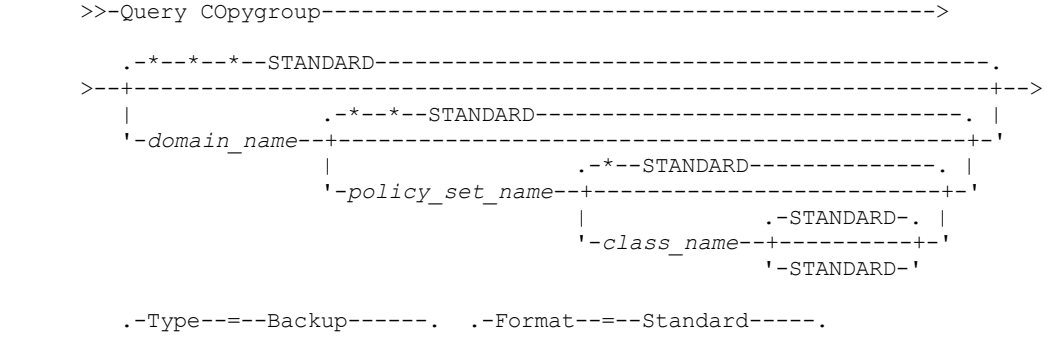
QUERY COPYGROUP (Query copy groups)

Use this command to display information about one or more copy groups.

Privilege class

Any administrator can issue this command.

Syntax



```
>--+----------------------+--+------------------------+------->
   '-Type--=--+-Backup--+-'  '-Format--=--+-Standard-+-'
              '-Archive-'                 '-Detailed-'
```

Parameters

domain_name
: Specifies the policy domain that is associated with the copy group to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all policy domains are queried. You must specify this parameter when querying an explicitly named copy group.

policy_set_name
: Specifies the policy set associated with the copy group to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all policy sets are queried. You must specify this parameter when querying an explicitly named copy group.

class_name
: Specifies the management class that is associated with the copy group to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all management classes are queried. You must specify this parameter when querying an explicitly named copy group.

STANDARD
: Specifies the name of the copy group. This parameter is optional. The name of the copy group must be STANDARD. The default is STANDARD.

Type
: Specifies the type of copy group to be queried. This parameter is optional. The default value is BACKUP. Possible values are:

  Backup
  : Specifies that you want to query backup copy groups.

  Archive
  : Specifies that you want to query archive copy groups.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display information about the default backup copy group

Display information about the default backup copy group in the ENGPOLDOM engineering policy domain. Issue the following command:

```
query copygroup engpoldom * *
```

The following data shows the output from the query. It shows that the ACTIVE policy set contains two backup copy groups that belong to the MCENG and STANDARD management classes.

```
Policy     Policy    Mgmt       Copy     Versions  Versions Retain   Retain
Domain     Set       Class      Group    Data      Data     Extra    Only
Name       Name      Name       Name     Exists    Deleted  Versions Version
---------- --------  --------   -------  --------  -------  -------  -------
ENGPOLDOM  ACTIVE    MCENG      STANDARD  5         4        90       600
ENGPOLDOM  ACTIVE    STANDARD   STANDARD  2         1        30       60
ENGPOLDOM  STANDARD  MCENG      STANDARD  5         4        90       600
ENGPOLDOM  STANDARD  STANDARD   STANDARD  2         1        30       60
ENGPOLDOM  TEST      STANDARD   STANDARD  2         1        30       60
```

Example: Display detailed information on one backup copy group

Display complete information on the backup copy group assigned to the ACTIVEFILES management class in the VACATION policy set of the EMPLOYEE_RECORDS policy domain. Issue the command:

```
query copygroup employee_records vacation
activefiles format=detailed
```

Example: Display information on the backup copy group in the STANDARD management class and policy set

From a managed server, display complete information on the backup copy group assigned to the STANDARD management class in the STANDARD policy set of the ADMIN_RECORDS policy domain. Issue the command:

```
query copygroup admin_records
standard standard format=detailed
```

```
                 Policy Domain Name: ADMIN_RECORDS
                    Policy Set Name: STANDARD
                    Mgmt Class Name: STANDARD
                    Copy Group Name: STANDARD
                    Copy Group Type: Backup
                Versions Data Exists: 2
               Versions Data Deleted: 1
               Retain Extra Versions: 30
                 Retain Only Version: 60
                           Copy Mode: Modified
                  Copy Serialization: Shared Static
                      Copy Frequency: 0
                    Copy Destination: BACKUPPOOL
Table of Contents (TOC) Destination:
     Last Update by (administrator): $$CONFIG_MANAGER$$
              Last Update Date/Time: 2002.10.02 17.51.49
                   Managing profile: ADMIN_INFO
                    Changes Pending: Yes
```

Example: Display information on an archive copy group

From a managed server, display complete information on the archive copy group STANDARD that is assigned to the MCLASS1 management class in the SUMMER policy set of the PROG1 policy domain. Issue the command:

```
query copygroup prog1 summer mclass1
type=archive format=detailed
```

```
                 Policy Domain Name: PROG1
                    Policy Set Name: SUMMER
                    Mgmt Class Name: MCLASS1
                    Copy Group Name: STANDARD
                    Copy Group Type: Archive
                     Retain Version: 730
               Retention Initiation: Creation
                  Minimum Retention:
                  Copy Serialization: Shared Static
                      Copy Frequency: Cmd
                           Copy Mode: Absolute
                    Copy Destination: ARCHPOOL
     Last Update by (administrator): $$CONFIG_MANAGER$$
              Last Update Date/Time: 2002.10.02 17.42.49
                   Managing profile: ADMIN_INFO
```

Example: Display information on the copy group for a NAS backup

Query the copy group for the NAS backup. Issue the command:

```
query copygroup nasdomain
type=backup
```

```
                 Policy Domain Name: NASDOMAIN
                    Policy Set Name: ACTIVE
                    Mgmt Class Name: STANDARD
                    Copy Group Name: STANDARD
                    Copy Group Type: Backup
                Versions Data Exists: 2
               Versions Data Deleted: 1
               Retain Extra Versions: 30
                 Retain Only Version: 60
                           Copy Mode: Modified
                  Copy Serialization: Shared Static
                      Copy Frequency: 0
```

```
                  Copy Destination: NASPOOL
Table of Contents (TOC) Destination: BACKUPPOOL
     Last Update by (administrator): SERVER_CONSOLE
              Last Update Date/Time: 10/02/2002 12:16:52
                   Managing profile:
                    Changes Pending: Yes
```

Field descriptions

Policy Domain Name
: The name of the policy domain.

Policy Set Name
: The name of the policy set.

Mgmt Class Name
: The name of the management class.

Copy Group Name
: The name of the copy group. This name is always STANDARD.

Copy Group Type
: The type of the copy group.

Versions Data Exists
: The maximum number of backup versions to retain for files that are currently on the client file system.

Versions Data Deleted
: The maximum number of backup versions to retain for files that have been deleted from the client file system after being backed up using IBM Spectrum Protect™.

Retain Extra Versions
: The number of days to retain a backup version after that version becomes inactive.

Retain Only Version
: The number of days to retain the last backup version of a file that has been deleted from the client file system.

Copy Serialization
: Whether a file can be in use during an archive operation.

Copy Frequency
: The copy frequency of the copy group. For archive copy groups, this value is always CMD.

Copy Mode
: Specifies that files in the copy group are archived regardless of whether they have been modified. For archive copy groups, this value is always ABSOLUTE.

Copy Destination
: The name of the storage pool where the server initially stores files associated with this archive copy group.

Table of Contents (TOC) Destination
: The name of the primary storage pool in which TOCs are initially stored for image backup operations in which TOC generation is requested.

Last Update by (administrator)
: The name of the administrator or server that most recently updated the copy group. If this field contains $$CONFIG_MANAGER$$, the copy group is associated with a domain that is managed by the configuration manager.

Last Update Date/Time
: The date and time when the copy group was most recently defined or updated.

Managing Profile
: The profile or profiles to which the managed server subscribed to get the definition of this policy copy group.

Changes Pending
: Whether or not changes are being made but not activated. Once the changes are activated, the field resets to No.

Related commands

Table 1. Commands related to QUERY COPYGROUP

Command	Description
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DELETE COPYGROUP	Deletes a backup or archive copy group from a policy domain and policy set.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

AIX | Linux | Windows

QUERY DAMAGED (Query damaged data in a directory-container or cloud-container storage pool)

Use this command to display information about damaged data extents in a directory-container or cloud-container storage pool. Use this command together with the AUDIT CONTAINER command to determine a recovery method for the damaged data.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query DAMaged--pool_name------------------------------------>

   .-Type--=--Status---------------.
>--+-------------------------------+--------------------------><
   '-Type--=--+-INVentory--------+-'
              +-Node--| A |------+
              '-CONTAiner--| A |-'

A (Additional filter by node name)

|--+------------------------+-----------------------------------|
   '-Nodename--=--node_name-'
```

Parameters

pool_name (Required)
: Specifies the name of the directory-container or cloud storage pool.

Type
: Specifies the type of information to display. This parameter is optional. Specify one of the following values:

  Status
  : Specifies that information is displayed about damaged data extents. For cloud storage pools, orphaned extents are also displayed. This is the default.

  Node
  : Specifies that information about the number of damaged files per node is displayed.

  INVentory
  : Specifies that inventory information for each damaged file is displayed.

  CONTAiner
  : Specifies that the containers that contain damaged data extents or cloud orphaned extents are displayed. For directory-container storage pools, storage pool directories are also displayed.

Nodename
: Specifies that damaged file information for a single node is displayed.
  Restriction: You cannot specify this parameter if the TYPE=CONTAINER or TYPE=STATUS parameter is specified.

Example: Display status information about damaged or orphaned data extents

Display information about the status of damaged data extents that are stored in a container.

```
query damaged pool1 type=status

Storage Pool     Non-Dedup Data    Dedup Data     Cloud Orphaned
Name             Extent Count      Extent Count   Extent Count
---------------  -------------     ----------     -------------
POOL1                  58               145
```

For cloud storage pools, the number of orphaned extents is also displayed.

```
Storage Pool     Non-Dedup Data    Dedup Data     Cloud Orphaned
Name             Extent Count      Extent Count   Extent Count
```

```
---------------  -------------     ----------     -------------
POOL1                   65               238           18
```

Example: Display information about a damaged file for a node type

Display information about damaged files that are stored in a node.

```
query damaged pool1 type=node

Node Name      Number of
               Damaged Files
-------------  -----------------
POOL1                   37
```

Example: Display information about a damaged file for an inventory type

Display information about damaged files that are stored in an inventory.

```
query damaged pool2 type=inventory

       Client's Name for File: /data/files/10.out
                         Type: Bkup
                    Node Name: NODE1
               Filespace Name: /data/space
                        State: Available
               Insertion time: 01/19/2015 16:01:35
                    Object ID: 2073
```

Example: Display information about a damaged file for a container type

Display information about damaged files that are stored in a container.

```
query damaged pool3 type=container

         Directory ID: 1
            Directory: /abc/space/container1
            Container: /abc/space/container1/00/0000000000000022.dcf
                State: Unavailable
```

For cloud containers, only the name of the container is displayed.

```
         Directory ID:
            Directory:
            Container: ibmsp.12520ae05b4011e613320a0027000000/
                       001-10006a3278bc34f0e4118a850090fa3dcb48/
                       00000000000001.ncf
                State:
```

For local storage, the following information about a damaged container is displayed.

```
               Directory ID: 1
                  Directory: localdirectory
                  Container: localdirectory/00/00000000000011.ncf
                      State: Unavailable
```

Field descriptions

Client's Name for File (TYPE=INVENTORY only)
: The name of the file.

Cloud Orphaned Extent Count (TYPE=STATUS only)
: The number of orphaned extents in a cloud storage pool. Extents are considered orphaned if they do not have a corresponding database entry.

Container (TYPE=CONTAINER only)
: The name of the container.

Deduplicated Extent Count (TYPE=STATUS only)
: The number of damaged extents in the storage pool for deduplicated data.

Directory (TYPE=CONTAINER only)

The name of the storage pool directory.

Directory ID (TYPE=CONTAINER only)
The identification number of the storage pool directory.

Filespace Name (TYPE=INVENTORY only)
The name of file space.

Insertion time (TYPE=INVENTORY only)
The date and time that the object was stored on the server.

Node Name (TYPE=INVENTORY or TYPE=NODE only)
The name of the node.

Non-Deduplicated Extent Count (TYPE=STATUS only)
The number of damaged extents in the storage pool for data that is not deduplicated, such as metadata and client-encrypted data.

Number of Damaged Files (TYPE=NODE only)
The number of damaged files per node.

Object ID (TYPE=INVENTORY only)
The identification number of the object.

State (TYPE=INVENTORY or TYPE=CONTAINER only)
The state of the data in either the inventory or the container, depending on the type of data you are querying. The field can contain one of the following values:

Active
The version of the file in the inventory is active. There can be only one active version of the file in the inventory.

Inactive
The version of the file in the inventory is inactive. There can be multiple inactive versions of the file in the inventory.

Available
The state of the container is available.

Unavailable
The state of the container is unavailable. For example, a container might be unavailable if the header is corrupted or if the container cannot be opened.

Read-Only
The container is in a read-only state. Data in the container can be read, but data cannot be written to the container.

Pending
The container is pending deletion. The contents of the container were moved to a different container, and the container is ready to be deleted.

Type (TYPE=INVENTORY only)
The type of data in the file.

Table 1. Commands related to QUERY DAMAGED

Command	Description
AUDIT CONTAINER	Audit a directory-container storage pool.
QUERY CLEANUP	Query the cleanup status of a source storage pool.
QUERY CONTAINER	Displays information about a container.
REMOVE DAMAGED	Removes damaged data from a source storage pool.

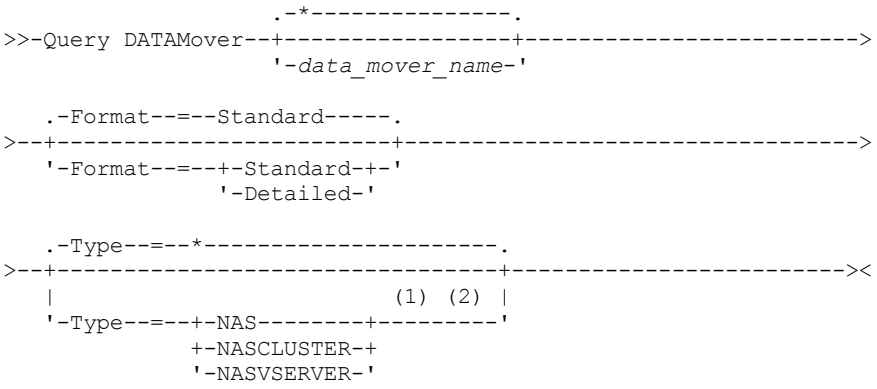
QUERY DATAMOVER (Display data mover definitions)

Use this command to display data mover definitions.

Privilege class

Any administrator can issue this command.

Syntax



Notes:

1. You must specify the TYPE parameter if `FORMAT=DETAILED`.
2. You can specify `TYPE=NASCLUSTER` and `TYPE=NASVSERVER` only on an AIX, Linux, or Windows operating system.

Parameters

data_mover_name
: Specifies the name of the data mover to display. You can specify multiple names with a wildcard character. The default displays all data movers.

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD.

  Standard
  : Specifies that name and address information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Type
: Specifies the type of data mover to be displayed. If you specify `FORMAT=DETAILED`, you must specify a value for the TYPE parameter.

  NAS
  : Specifies a NAS file server.

  AIX Linux Windows NASCLUSTER
  : AIX Linux Windows Specifies a clustered NAS file server.

  AIX Linux Windows NASVSERVER
  : AIX Linux Windows Specifies a virtual storage device within a cluster.

Example: Display information about all data movers

Display the data movers on the server. Issue the command:

```
query datamover
```

```
Data Mover Name    Data Mover Type     Online
-------------      -------------       ------
 NASMOVER1              NAS               Yes
 NASMOVER2              NAS                No
```

See Field descriptions for field descriptions.

Example: Display information about one data mover

Display partial information about data mover DATAMOVER6. Issue the command:

```
query datamover datamover6 type=nas
```

```
 Source Name       Type           Online
-------------      -------        ------
```

```
DATAMOVER6        NAS             Yes
```

See Field descriptions for field descriptions.

Example: Display detailed information about one data mover

Display detailed information about data mover DATAMOVER6. The TYPE parameter is required when FORMAT=DETAILED. Issue the command:

```
query datamover datamover6 format=detailed type=nas
```

```
               Data Mover Name:   DataMover6
               Data Mover Type:   NAS
                    IP Address:   198.51.100.0
           TCP/IP Port Number:   10000
                     User Name:   NDMPadmin
     Storage Pool Data Format:   NDMPDUMP
                       Online:   Yes
Last Update by (administrator):   ADMIN
        Last Update Date/Time:   05/23/2015 09:26:33
```

See Field descriptions for field descriptions.

AIX | Linux | Windows

Example: Display detailed information about a clustered NAS data mover

Display detailed information about a clustered NAS data mover that is named CLUSTERA. Issue the following command:

```
query datamover clustera format=detailed type=nascluster
```

```
               Data Mover Name:   CLUSTERA
               Data Mover Type:   NASCLUSTER
                    IP Address:   192.0.2.255
           TCP/IP Port Number:   10000
                     User Name:   ndmp
     Storage Pool Data Format:   NETAPPDUMP
                       Online:   Yes
Last Update by (administrator):   ADMIN
        Last Update Date/Time:   04/28/2015 09:26:33
```

See Field descriptions for field descriptions.

Field descriptions

Data Mover Name
: Specifies the name of the data mover.

Data Mover Type
: Specifies the type of the data mover.

IP Address
: Specifies the IP address of the data mover.

TCP/IP Port Number
: Specifies the TCP port number for the data mover.

User Name
: Specifies the user ID that the server uses to access the data mover.

Storage Pool Data Format
: Specifies the data format that is used by the data mover.

Online
: Specifies whether the data mover is online and available for use.

Last Update by (administrator)
: Specifies the ID of the administrator who completed the last update.

Last Update Date/Time
: Specifies the date and time when the last update occurred.

Related commands

Table 1. Commands related to QUERY DATAMOVER

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DELETE DATAMOVER	Deletes a data mover.
UPDATE DATAMOVER	Changes the definition for a data mover.

QUERY DB (Display database information)

Use this command to display information about the database.

Privilege class

Any administrator can issue this command.

Syntax

```
             .-Format--=--Standard-----.
>>-Query DB--+-------------------------+----------------------><
             '-Format--=--+-Standard-+-'
                          '-Detailed-'
```

Parameters

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. The following values are possible:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display summary statistics about the database

Display statistical information about the database. Issue the command:

```
query db
```

```
Database Name  Total Pages  Usable Pages  Used Pages  Free Pages
-------------  -----------  ------------  ----------  ----------
       TSMDB1       32,776        32,504      24,220       8,284
```

See Field descriptions for field descriptions.

Example: Display detailed database information

Display detailed statistical information about the database. Issue the command:

```
query db format=detailed
```

```
                  Database Name: TSM_DB2
  Total Space of File System (MB): 1,748,800
   Space Used on File System (MB): 2,304,355
      Space Used by Database (MB): 448
        Free Space Available (MB): 235,609
                     Total Pages: 32,776
                    Usable Pages: 32,504
                      Used Pages: 24,220
                      Free Pages: 8,284
            Buffer Pool Hit Ratio: 99.3
            Total Buffer Requests: 204,121
                   Sort Overflows: 0
          Package Cache Hit Ratio: 89.8
```

```
     Last Database Reorganization: 05/25/2009 16:44:06
           Full Device Class Name: FILE
Number of Database Backup Streams: 4
     Incrementals Since Last Full: 0
   Last Complete Backup Date/Time: 05/18/2009 22:55:19
        Compress Database Backups: Yes
    Protect Master Encryption Key: No
```

See Field descriptions for field descriptions.

Field descriptions

Database Name
: The name of the database that is defined and configured for use by the IBM Spectrum Protect™ server.

AIX Linux Total Space of File System (MB)
: AIX Linux The total space, in megabytes, of the file systems in which the database is located.

Windows Total Space of File System (MB)
: Windows The total space, in megabytes, of the drives on which the database is located.

Space Used on File System (MB)
: The amount of database space, in megabytes, that is in use.

Space Used by Database (MB)
: The size of the database, in megabytes. The value does not include any temporary table space. The size of the database is calculated from the amount of space that is used on the file system containing the database.

Free Space Available (MB)
: The amount of database space, in megabytes, that is not in use.

Total Pages
: The total number of pages in the table space.

Usable Pages
: The number of usable pages in the table space.

Used Pages
: The number of used pages in the table space.

Free Pages
: The total number of free pages in all table spaces. The IBM Spectrum Protect database has up to 10 table spaces.

Buffer Pool Hit Ratio
: The total hit ratio percent.

Total Buffer Requests
: The total number of buffer pool data logical reads and index logical reads since the last time the database was started or since the database monitor was reset.

Sort Overflows
: The total number of sorts that ran out of the sort heap and might have required disk space for temporary storage.

Package Cache Hit Ratio
: A percentage that indicates how well the package cache is helping to avoid reloading packages and sections for static SQL from the system catalogs. It also indicates how well the package cache is helping to avoid recompiling dynamic SQL statements. A high ratio indicates that it is successful in avoiding these activities.

Last Database Reorganization
: The last time that the database manager completed an automatic reorganization activity.

Full Device Class Name
: The name of the device class that is used for full database backups.

Number of Database Backup Streams
: The number of concurrent data movement streams that were used during the database backup.

Incrementals Since Last Full
: The number of incremental backups that were completed since the last full backup.

Last Complete Backup Date/Time
: The date and time of the last full backup.

Compress Database Backups
: Specifies whether database backups are compressed.

Protect Master Encryption Key
: Specifies whether database backups include a copy of the server master encryption key.

Related commands

Table 1. Commands related to QUERY DB

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
EXTEND DBSPACE	Adds directories to increase space for use by the database.
QUERY DBSPACE	Displays information about the storage space defined for the database.

QUERY DBSPACE (Display database storage space)

Use this command to display information about the directories used by the database to store data.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-QUERY DBSpace-------------------------------------------------><
```

Parameters

None.

Example: Display database storage space information

Display information about database storage space. Issue the command:

```
query dbspace
```

AIX Linux

```
Location            Total Space of     Used Space on     Free Space
                    File System (MB)   File System (MB)  Available (MB)
-----------------   ----------------   ---------------   --------------
/tsmdb001           1,748,800          1,513,191.125     117,804.422
/tsmdb002           1,748,800          1,513,191.125     117,804.422
```

Windows

```
Location            Total Space of     Used Space on     Free Space
                    File System (MB)   File System (MB)  Available (MB)
-----------------   ----------------   ---------------   --------------
d:\tsm\db001        1,748,800          1,513,191.125     117,804.422
e:\tsm\db002        1,748,800          1,513,191.125     117,804.422
```

See Field descriptions for field descriptions.

Field descriptions

Location
: Specifies the locations of database directories.

AIX Total Space of File System (MB)
: AIX The total amount of space, in megabytes, of the file system in which the database is located.

Windows Total Space of File System (MB)
: Windows The total amount of space, in megabytes, of the drives on which the database is located.

Used Space on File System (MB)
: The amount of storage space, in megabytes, that is in use.

  AIX Linux When you run the QUERY DBSPACE command, the value in the output might be greater than the value that is obtained by running the df system command. The output from the df system command does not include the amount of space that is reserved for the root user.

Linux If you run the df system command, the default percentage of space that is reserved for the root user is 5%. You can change this default value.

Free Space Available (MB)
The amount of space, in megabytes, that is not in use.

Windows Free Space Available (MB)
Windows The amount of space remaining on the drive where the directory is located.

Related commands

Table 1. Commands related to QUERY DBSPACE

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
EXTEND DBSPACE	Adds directories to increase space for use by the database.
QUERY DB	Displays allocation information about the database.

AIX Linux Windows

QUERY DEDUPSTATS (Query data deduplication statistics)

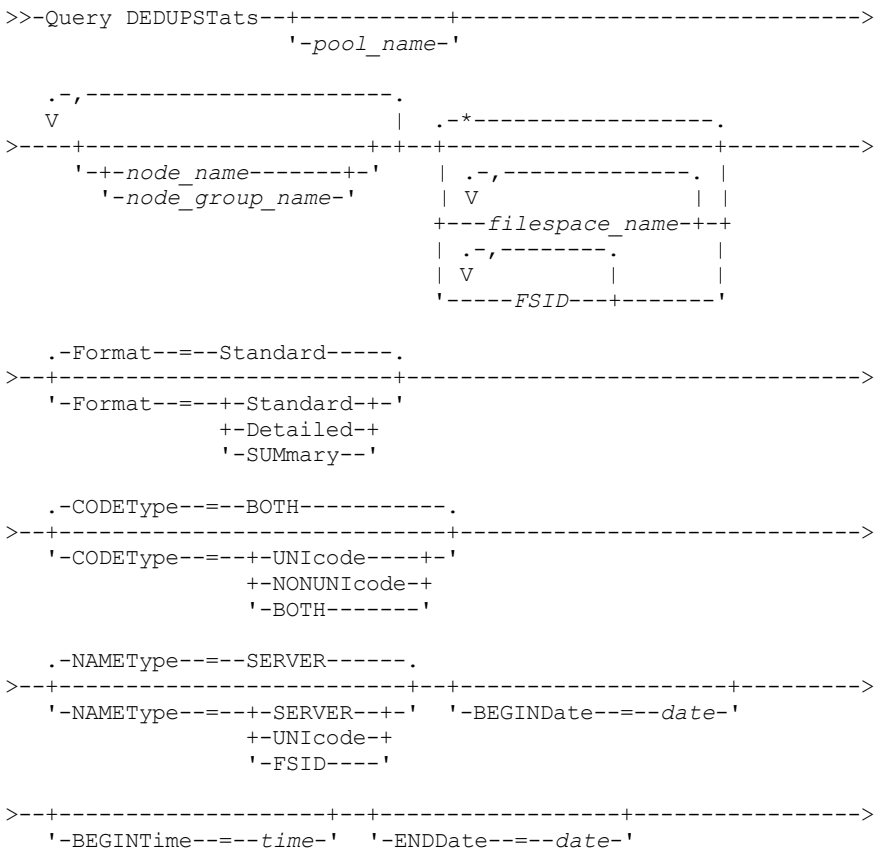
Use this command to display information about data deduplication statistics for a directory-container storage pool or a cloud storage pool. You can display statistics for an entire storage pool or for data from a specified group of client nodes.

You must issue the GENERATE DEDUPSTATS command before you can issue the QUERY DEDUPSTATS command.

Privilege class

Any administrator can issue this command.

Syntax



```
                        .-ALLSTats---=--No------.
>--+-------------------+--+----------------------+---------------->
   '-ENDTime---=--time-'  '-ALLSTats---=--+-Yes-+-'
                                          '-No--'

   .-REPortid--=--report_id-.
>--+------------------------+-------------------------------------->

>--+----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

pool_name
: Specifies the name of the directory-container storage pool whose data is contained in the data deduplication statistics. This parameter is optional. If you do not specify a value for this parameter, all storage pools are displayed. You can specify up to 30 characters for the storage pool name. If you specify more than 30 characters, the command fails.
Restriction: You can specify directory-container storage pools or cloud storage pools only.

node_name or node_group_name
: Specifies the name of the client node or defined group of client nodes that is reported in the data deduplication statistics. You can also specify a combination of client node names and client-node group names. This parameter is optional. To specify multiple client node names or client-node group names, separate the names with commas with no intervening spaces. You can use wildcard characters with client node names but not with client-node group names. The specified value can have a maximum of 1024 characters.

filespace_name or FSID
: Specifies the names of one or more file spaces that contain the data to be included in the data deduplication statistics. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, all file spaces are displayed. You can specify more than one file space by separating the names with commas and no intervening spaces. The specified value can have a maximum of 1024 characters.
For a server that has clients with support for file spaces that are in Unicode format, you can enter either a file space name or a file space identifier (FSID). If you enter a file space name, you might need to have the server convert the file space name that you enter. For example, you might need to have the server convert the name that you enter from the server's code page to Unicode.
Restrictions: The following restrictions apply to file space names and FSIDs:

- You must specify a node name if you specify a file space name.
- Do not mix file space names and FSIDs in the same command.

Format
: Specifies how the information is displayed. This parameter is optional. Specify one of the following values:

  Standard
  : Specifies that partial information is displayed for the specified data deduplication sets. This is the default.

  Detailed
  : Specifies that complete information is displayed for the specified data deduplication sets.

  SUMmary
  : Specifies that summarized status is displayed for data deduplication sets that are in the same group, as defined by the REPORTID parameter.

CODEType
: Specify what type of file spaces to include in the operation. The default value is BOTH, which specifies that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name. Specify one of the following values:

  UNIcode
  : Include file spaces that are in Unicode format.

  NONUNIcode
  : Include file spaces that are not in Unicode format.

  BOTH
  : Include file spaces regardless of code page type. This is the default.

NAMEType

Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for file spaces that are in Unicode format. You can use this parameter for IBM Spectrum Protect™ clients that use Windows, NetWare, or Macintosh OS X operating systems.
Use this parameter only when you enter a node name and a file space name or FSID.
Restriction: When you specify this parameter, the file space name cannot contain a wildcard.

Specify one of the following values:

SERVER
: The server uses the server's code page to interpret the file space names. This is the default.

UNIcode
: The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

FSID
: The server interprets the file space names as their FSIDs.

BEGINDate
: Specifies the start date to query data deduplication statistics. This parameter is optional. You can use this parameter with the BEGINTIME parameter to specify a range for the date and time. If you specify a begin date without a begin time, the time is at 12 midnight on the date you specify.
Restriction: You can specify this parameter only when you specify the ALLSTATS=YES parameter.
Specify one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date.	09/15/2015
TODAY	The current date.	TODAY
TODAY-days or days	The current date minus days specified.	TODAY -3 or -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include records that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include records that were active on the 10th day of the current month.

BEGINTime
: Specifies the start time to query the data deduplication statistics. This parameter is optional. You can use this parameter with the BEGINDATE parameter to specify a range for the date and time. If you specify a begin time without a begin date, the date is the current date at the time you specify.
Restriction: You can specify this parameter only when you specify the ALLSTATS=YES parameter.
Specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	10:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus hours and minutes specified.	NOW+02:00 or +02:00.
NOW-HH:MM or-HH:MM	The current time minus hours and minutes specified.	NOW-02:00 or –02:00.

ENDDate
: Specifies the end date to query data deduplication statistics. This parameter is optional. You can use this parameter with the ENDTIME parameter to specify a range for the date and time. If you specify an end date without an end time, the time is

at 11:59:59 p.m. on the specified end date.
Restriction: You can specify this parameter only when you specify the ALLSTATS=YES parameter.
Specify one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY-days or -days	The current date minus days specified.	TODAY -3 or -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include records that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include records that were active on the 10th day of the current month.

ENDTime
Specifies the end time of the range to query the data deduplication statistics. This parameter is optional. You can use this parameter with the ENDDATE parameter to specify a range for the date and time. If you specify an end time without an end date, the date is the current date at the time you specify.
Restriction: You can specify this parameter only when you specify the ALLSTATS=YES parameter.
Specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	10:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus hours and minutes on the specified end date	NOW+02:00 or +02:00.
NOW-HH:MM or -HH:MM	The current time minus hours and minutes on the specified end date	NOW-02:00 or -02:00.

ALLSTats
Specifies whether to display all data deduplication statistics or only the most recently generated data deduplication statistics. This parameter is optional. Specify one of the following values:

No
Displays only data deduplication statistics that were most recently generated for each node and file space.
Yes
Displays all data deduplication statistics.

REPortid
Specifies an ID for a set of data deduplication statistics that is generated on a specific day for specified nodes, file spaces, or both. For example, if you generate statistics on 30 September 2018 for a node list (TEST1, TEST2, TEST3, and MYGROUP1) and a file space list (FS1, FS2, and /tmp*), a report ID (for example, 1) is assigned to that set. If statistics are generated for the same nodes and file spaces on the next day, a new report ID (for example, 2) is assigned to that set. This parameter is optional.

DESCription
Specifies a description of the generated statistics. This parameter is optional.

Example: View data deduplication statistics in standard format

Display data deduplication statistics for a storage pool that is named POOL1. The data deduplication statistics are for node NODE1 and the statistics from 8 May 2015 are displayed. See Field descriptions for field descriptions.

```
query dedupstats pool1 node1 begindate=05/08/2015
```

```
                        Date/Time: 05/05/2015 15:15:23
                Storage Pool Name: POOL1
                        Node Name: NODE1
                   Filespace Name: \\fs1\a1
                             FSID: 41
                             Type: Bkup
          Total Saving Percentage: 86.62
        Total Data Protected (MB): 311
```

Example: View detailed data deduplication statistics

Display detailed information for data deduplication for a storage pool that is named POOL1.

```
query dedupstats pool1 format=detailed
```

```
                        Date/Time: 05/05/2015 15:15:23
                Storage Pool Name: POOL1
                        Node Name: NODE1
                   Filespace Name: \\fs1\a1
                             FSID: 41
                             Type: Bkup
        Total Data Protected (MB): 47,646
            Total Space Used (MB): 10,139
           Total Space Saved (MB): 37,507
          Total Saving Percentage: 78.72
            Deduplication Savings: 16,228,107,499
         Deduplication Percentage: 42.59
     Non-Deduplicated Extent Count: 1,658
Non-Deduplicated Extent Space Used: 732,626
               Unique Extent Count: 189,791
          Unique Extent Space Used: 23,385,014,635
               Shared Extent Count: 178,712
      Shared Extent Data Protected: 26,575,010,669
          Shared Extent Space Used: 5,267,815,421
               Compression Savings: 5,267,815,421
         Compression Percentage: 62.93
          Compressed Extent Count: 352,498
       Uncompressed Extent Count: 17,663
      Encryption Extent Space Used: 52,901,672
             Encryption Percentage: 100.00
           Encrypted Extent Count: 188
         Unencrypted Extent Count: 0
                        Report ID: 1
                      Description:
```

Example: View summarized data deduplication statistics

Display a summary of information for a set of statistics.

```
query dedupstatus reportid=1234 format=summary
```

```
                        Report ID: 1234
                      Description:
                        Date/Time: 09/15/2017 16:59:55
                Storage Pool Name: DIRPOOL
                        Node Name: TEST1,TEST2,TEST3,MYGROUP1
                   Filespace Name: FS1,FS2,/tmp*
                             Type: Bkup
        Total Data Protected (MB): 47,646
            Total Space Used (MB): 10,139
           Total Space Saved (MB): 37,507
          Total Saving Percentage: 78.72
            Deduplication Savings: 16,228,107,499
         Deduplication Percentage: 42.59
     Non-Deduplicated Extent Count: 1,658
Non-Deduplicated Extent Space Used: 732,626
               Unique Extent Count: 189,791
          Unique Extent Space Used: 23,385,014,635
               Shared Extent Count: 178,712
      Shared Extent Data Protected: 26,575,010,669
          Shared Extent Space Used: 5,267,815,421
               Compression Savings: 5,267,815,421
```

```
          Compression Percentage: 62.93
        Compressed Extent Count: 352,498
     Uncompressed Extent Count: 17,663
Encryption Extent Space Used: 52,901,672
         Encryption Percentage: 100.00
       Encrypted Extent Count: 188
    Unencrypted Extent Count: 0
```

Field descriptions

Report ID
: An ID for a set of data deduplication statistics that is generated on a specific day for a specified group of nodes, file spaces, or both.

Description
: A description of the statistics set that is generated.

Date/Time
: The time and date that the data deduplication statistics are generated.

Storage Pool Name
: The name of the storage pool.

Node Name
: The name of the client node whose data is contained in the data deduplication statistics.

Filespace Name
: The name of the file space.

FSID
: The name of the file space identifier.

Type
: The type of data. The following values are possible:

  Arch
  : Data that is archived.

  Bkup
  : Data that is backed up.

  SpMg
  : Data that is migrated from an IBM Spectrum Protect for Space Management client.

Total Data Protected (MB)
: The logical amount of data, in megabytes, that is protected in the storage pool before data deduplication and compression. This value represents the sum of the Total Space Used (MB) and Total Space Saved (MB) values.

Total Space Used (MB)
: The total amount of used space in the storage pool, in megabytes. This value is the physical amount of data that is backed up after data deduplication and compression.

Total Space Saved (MB)
: The total amount of space, in megabytes, of data that is removed from the storage pool because of data deduplication and compression. This value represents the sum of the Deduplication Savings and Compression Savings values.

Total Saving Percentage
: The percentage of data that is removed from the storage pool because of compression and data deduplication.

Deduplication Savings
: The amount of used space that is saved in the storage pool because of data deduplication.

Deduplication Percentage
: The percentage of data that is removed from the storage pool because of data deduplication.

Non-Deduplicated Extent Count
: The number of data extents that are not deduplicated in the storage pool.

Non-Deduplicated Extent Space Used
: The amount of space that is used by data extents that are not deduplicated in the storage pool. This value applies to containers that have a .ncf file type and that do not have deduplicated data.
  Tip: Data extents that are not deduplicated consist of the following data or file types:

  - File metadata.
  - Files that are less than 2 KB.
  - Files that use client encryption.

Unique Extent Count

The number of data extents that are not shared by a node.

Unique Extent Space Used
: The amount of space in the storage pool that is not shared by a node. This value applies to containers that have a .dcf file type and that do not have deduplicated data.

Shared Extent Count
: The number of data extents that are used multiple times by the same node or by different nodes because of data deduplication.

Shared Extent Data Protected
: The amount of space in the storage pool that is protected by shared data extents before data deduplication.

Shared Extent Space Used
: The amount of space in the storage pool that is used by shared data extents after data deduplication.

Compression Savings
: The amount of used space that is saved in the storage pool because of compression after data deduplication.

Compression Percentage
: The percentage of data that is removed from the storage pool because of compression.

Compressed Extent Count
: The number of data extents that are compressed.

Uncompressed Extent Count
: The number of data extents that are uncompressed.

Encryption Extent Space Used
: The amount of space in the storage pool that is used by encrypted data extents.

Encryption Percentage
: The percentage of encrypted data in the storage pool.

Encrypted Extent Count
: The number of data extents that are encrypted.

Unencrypted Extent Count
: The number of data extents that are not encrypted.

Related commands

Table 1. Commands related to QUERY DEDUPSTATS

Command	Description
DELETE DEDUPSTATS	Deletes data deduplication statistics.
GENERATE DEDUPSTATS	Generates data deduplication statistics.

QUERY DEVCLASS (Display information on one or more device classes)

Use this command to display information on one or more device classes.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*-----------------.
>>-Query DEVclass--+-------------------+------------------------>
                    '-device_class_name-'

   .-Format--=--Standard-----.
>--+------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

device_class_name
: Specifies the name of the device class to be queried. This parameter is optional. You can use wildcard characters to specify this name. All matching device classes are displayed. If you do not specify a value for this parameter, all device classes are

displayed.

Format

Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

Standard

Specifies that partial information is displayed for the specified device class.

Detailed

Specifies that complete information is displayed for the specified device class.

Example: List all device classes

Display information on all device classes.

```
query devclass
```

AIX Linux Windows

```
Device       Device     Storage  Device Format  Est/Max  Mount
Class        Access        Pool  Type           Capacity Limit
Name         Strategy     Count                    (MB)
-----------  ---------- -------  ------ ------  -------- -----
8MMTAPE      Sequential       1  8MM    DRIVE    6,144.0     2
DISK         Random           4
PLAINFILES   Sequential       1  FILE              50.0     1
8MMSP2       Sequential       2  8MM    DRIVE      44.4 DRIVES
```

See Field descriptions for field descriptions.

Example: Display detailed information for a specific FILE device class

Display information in full detail on the PLAINFILES device class.

```
query devclass plainfiles format=detailed
```

```
            Device Class Name: PLAINFILES
       Device Access Strategy: Sequential
           Storage Pool Count: 1
                  Device Type: FILE
                       Format:
        Est/Max Capacity (MB): 50.0
                  Mount Limit: 1
             Mount Wait (min):
       Mount Retention (min):
                Label Prefix:
```

Windows

```
                        Drive Letter:
                     Library:
                   Directory:
                  Server Name:
                 Retry Period:
               Retry Interval:
```

AIX Linux Windows

```
                                    Shared:
```

AIX Linux

```
                 Primary Allocation (MB):
    Secondary Allocation (MB):
                  Compression:
                    Retention:
                   Protection:
              Expiration Date:
                         Unit:
     Logical Block Protection:
Last Update by (administrator): ADMIN
        Last Update Date/Time: 05/31/2000 13:15:36
```

See Field descriptions for field descriptions.

Example: Display detailed information for a specific 3592 device class

Display full details on the 3592 device class.

```
query devclass 3592 format=detailed
```

```
            Device Class Name: 3592
       Device Access Strategy: Sequential
           Storage Pool Count: 1
                  Device Type: 3592
                       Format: 3592
        Est/Max Capacity (MB):
                  Mount Limit: DRIVES
             Mount Wait (min): 60
       Mount Retention (min): 60
                Label Prefix: ADSM
```
Windows
```
                 Drive Letter:
                      Library: MANLIB
                    Directory:
                  Server Name:
                 Retry Period:
               Retry Interval:
```
AIX Linux Windows
```
                       Shared:
                High-level Address:
                     WORM: No
             Scaled Capacity: 90
            Drive Encryption: On
```
AIX Linux
```
          Primary Allocation (MB):
    Secondary Allocation (MB):
                 Compression:
                   Retention:
                  Protection:
             Expiration Date:
                        Unit:
     Logical Block Protection: Read/Write
Last Update by (administrator): SERVER_CONSOLE
        Last Update Date/Time: 08/04/03 14:28:31
```

See Field descriptions for field descriptions.

Field descriptions

Device Class Name
: The name of the device class.

Device Access Strategy
: How data is written to the device class.

Storage Pool Count
: The number of storage pools that are assigned to the device class.

Device Type
: The device type of the device class.

Format
: The recording format.

Est/Max Capacity (MB)
: The estimated or maximum capacity of a volume that is associated with the device class.

Mount Limit
: The maximum number of sequential access volumes that can be mounted concurrently or specifies that DRIVES is the mount limit.

Mount Wait (min)
: The maximum number of minutes to wait for a sequential access volume to be mounted.

Mount Retention (min)
: The number of minutes to retain an idle sequential access volume before dismounting it.

Label Prefix
: The high-level qualifier of the data set name that the server writes into the sequential access media labels.

Windows Drive Letter
: Windows The drive letter for a removable file.

Library
: The name of the defined library object that contains the drives that are used by the device class.

Directory
: The directory or directories for a shared FILE device class.

Server Name
: The name of a defined server.

Retry Period
: The interval over which the server attempts to contact a target server if communications failure is suspected.

Retry Interval
How often the retries are done within a retry period.
Shared
Whether this FILE device class is shared between the server and one or more storage agents.
High-level Address
The IP address of the device in dotted decimal format.
Minimum Capacity
The minimum capacity of a volume that is associated with the device class.
WORM
Whether this drive is a write once, read many (WORM) device.
Drive Encryption
Whether drive encryption is allowed. This field applies only to volumes in a storage pool that is associated with a device type of 3592, LTO, or ECARTRIDGE.
Scaled Capacity
The percentage of the media capacity that can be used to store data.
AIX Linux Primary Allocation (MB)
AIX Linux For FILE device classes that represent storage that is managed by a z/OS® media server. Specifies the initial amount of space that is dynamically allocated when a new volume is opened.
AIX Linux Secondary Allocation (MB)
AIX Linux For FILE device classes that represent storage that is managed by a z/OS media server. Specifies the amount of space by which a file volume is extended when space that is already allocated to the file volume is used up.
AIX Linux Compression
AIX Linux For tape device classes that represent storage that is managed by a z/OS media server. Specifies whether the data is compressed.
AIX Linux Retention
AIX Linux For tape device classes that represent storage that is managed by a z/OS media server. Specifies the number of days to retain the tape, if retention is used.
AIX Linux Protection
AIX Linux For tape device classes that represent storage that is managed by a z/OS media server. Specifies whether the volumes are protected by the RACF program.
AIX Linux Expiration Date
AIX Linux For tape device classes that represent storage that is managed by a z/OS media server. Specifies the expiration date that is placed on the tape labels for this device class, if expiration is used.
AIX Linux Unit
AIX Linux For tape device classes that represent storage that is managed by a z/OS media server. Specifies the esoteric unit name for the group of tape devices.
Logical Block Protection
Specifies whether logical block protection is enabled and, if it is, the mode. Possible values are Read/Write, Write-only, and No. You can use logical block protection only with the following types of drives and media:

- IBM® LTO5 and later
- IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later
- Oracle StorageTek T10000C and T10000D drives

Last Update by (administrator)
The administrator that made the last update to the device class.
Last Update Date/Time
The date and time of the last update.

Related commands

Table 1. Commands related to QUERY DEVCLASS

Command	Description
DEFINE DEVCLASS	Defines a device class.
AIX Linux DEFINE DEVCLASS (z/OS media server)	AIX Linux Defines a device class to use storage managed by a z/OS media server.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE DEVCLASS	Deletes a device class.
QUERY DIRSPACE	Displays information about FILE directories.

Command	Description
QUERY SERVER	Displays information about servers.
UPDATE DEVCLASS	Changes the attributes of a device class.
AIX Linux UPDATE DEVCLASS (z/OS media server)	AIX Linux Changes the attributes of a device class for storage managed by a z/OS media server.

QUERY DIRSPACE (Query storage utilization of FILE directories)

Use this command to display information about free space in the directories associated with a device class with a device type of FILE.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query DIRSPace--+-------------------+----------------------><
                   '-device_class_name-'
```

Parameters

device_class_name
: Specifies the name of the device class to be queried. This parameter is optional. You can use wildcard characters to specify this name. All matching device classes of device type FILE are displayed. If you do not specify a value for this parameter, all device classes of device type FILE are displayed.

Example: List FILE type device classes

Display information for all device classes with a device type of FILE. In the following example the unit M is equivalent to megabytes, and the unit G is equivalent to gigabytes.

```
query dirspace
```

Windows

```
Device       Directory                     Estimated   Estimated
Class                                       Capacity   Available
-----------  ----------------------------  ----------  ----------
DBBKUP       /This/is/a/large/directory      13,000 M     5,543 M
DBBKUP       /This/is/directory2            13,000 M     7,123 M
DBBKUP2      /This/is/a/huge/directory        2,256 G     2,200 G
```

Windows

```
Device       Directory                     Estimated   Estimated
Class                                       Capacity   Available
-----------  ----------------------------  ----------  ----------
DBBKUP       G:\This\is\a\large\directory    13,000 M     5,543 M
DBBKUP       G:\This\is\directory2           13,000 M     7,123 M
DBBKUP2      G:\This\is\a\huge\directory       2,256 G     2,200 G
```

Field descriptions

Device Class Name
: The name of the device class.

Directory
: The path of the directory located on the server.

Estimated Capacity
: The estimated total capacity for the directory.

Estimated Available

The estimated remaining available space for the directory.

Related commands

Table 1. Commands related to QUERY DIRSPACE

Command	Description
DEFINE DEVCLASS	Defines a device class.
DELETE DEVCLASS	Deletes a device class.
QUERY DEVCLASS	Displays information about device classes.
UPDATE DEVCLASS	Changes the attributes of a device class.

QUERY DOMAIN (Query a policy domain)

Use this command to display information on one or more policy domains.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-*-----------.  .-Format--=--Standard-----.
>>-Query DOmain--+-------------+--+-------------------------+--><
                '-domain_name-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'
```

Parameters

domain_name
: Specifies the policy domain to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all policy domains are displayed.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display a summary of policy domains

Display partial information for all policy domains on the server. Issue the command:

```
query domain
```

```
Policy       Activated    Activated     Number of    Description
Domain       Policy       Default      Registered
Name         Set          Mgmt              Nodes
                          Class
---------    ---------    ---------    ----------    -----------------
EMPLOYEE-    VACATION     ACTIVEFI-             6    Employee Records
 _RECORDS                  LES                       Domain
PROG1                                           0    Programming Group
                                                       Test Domain
PROG2                                           0    Programming Group
                                                       Test Domain
STANDARD     STANDARD     STANDARD               1    Installed default
                                                       policy domain
```

See Field descriptions for field descriptions.

Example: Display the list of active-data pools

Display the active-data pool list. Issue the command:

```
query domain format=detailed
```

```
              Policy Domain Name: STANDARD
           Activated Policy Set: STANDARD
           Activation Date/Time: 05/16/2006 16:18:05
          Days Since Activation: 15
    Activated Default Mgmt Class: STANDARD
      Number of Registered Nodes: 1
                     Description: Installed default policy domain.
 Backup Retention (Grace Period): 30
Archive Retention (Grace Period): 365
  Last Update by (administrator): SERVER_CONSOLE
          Last Update Date/Time: 05/31/2006 15:17:48
               Managing profile:
                Changes Pending: Yes
          Active Data Pool List: ADPPOOL
```

See Field descriptions for field descriptions.

Field descriptions

Policy Domain Name
: The name of the policy domain.

Activated Policy Set
: The name of the policy set that was last activated in the domain.

  The definitions in the last activated policy set and the ACTIVE policy set are not necessarily identical. When you activate a policy set, the server copies the contents of the policy set to the policy set with the special name ACTIVE. The copied definitions in the ACTIVE policy set can be modified only by activating another policy set. You can modify the original policy set without affecting the ACTIVE policy set. Therefore, definitions in the policy set that was last activated might not be the same as those in the ACTIVE policy set.

Activation Date/Time
: The date and time that the policy set was activated.

Days Since Activation
: The number of days since the policy set was activated.

Activated Default Mgmt Class
: The assigned default management class for the policy set.

Number of Registered Nodes
: The number of client nodes registered to the policy domain.

Description
: The description of the policy domain.

Backup Retention (Grace Period)
: The number of days to retain inactive backup versions of files when any of the following conditions occur:

  - A file is rebound to a new management class, but neither the new management class nor default management class contains a backup copy group.
  - The management class to which a file is bound no longer exists, and the default management class does not contain a backup copy group.
  - The backup copy group is deleted from the management class to which a file is bound and the default management class does not contain a backup copy group.

Archive Retention (Grace Period)
: The number of days to retain an archive file that meets either of the following conditions:

  - The management class to which a file is bound no longer exists, and the default management class does not contain an archive copy group.
  - The archive copy group is deleted from the management class to which a file is bound and the default management class does not contain an archive copy group.

Last Update by (administrator)

The administrator that defined or most recently updated the policy domain. If this field contains $$CONFIG_MANAGER$$, the policy domain is associated with a profile that is managed by the configuration manager.

Last Update Date/Time
: When the administrator defined or most recently updated the policy domain.

Managing Profile
: The profile or profiles to which the managed server subscribed to get the definition of this policy domain.

Changes Pending
: Whether or not changes are being made but not activated. Once the changes are activated, the field resets to No.

Active Data Pool List
: The list of active-data pools in the domain.

Related commands

Table 1. Commands related to QUERY DOMAIN

Command	Description
COPY DOMAIN	Creates a copy of a policy domain.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DELETE DOMAIN	Deletes a policy domain along with any policy objects in the policy domain.
UPDATE DOMAIN	Changes the attributes of a policy domain.

QUERY DRIVE (Query information about a drive)

Use this command to display information about the drives associated with a library.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-*--*-------------------------.
>>-Query DRive--+-------------------------------+----------------><
                |               .-*----------. |
                '-library_name--+------------+-'
                                '-drive_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

library_name
: Specifies the name of the library where the queried drive is located. This parameter is optional. You can use a wildcard character to specify this name.

  You must specify a value for this parameter if you specify a drive name.

drive_name
: Specifies the name assigned to the drive. This parameter is optional. You can use a wildcard character to specify this name. If you specify a drive name, you must also specify a *library_name*.

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the drive.

  Detailed

Specifies that complete information is displayed for the drive.

Example: List drives associated with the server

Display information about all drives associated with the server. Issue the command:

```
query drive
```

```
Library    Drive     Device    Online
Name       Name      Type
--------   ------    --------  -----
LIB1       DRIVE01   3590       Yes
LIB2       DRIVE02   3590       Yes
```

See Field descriptions for field descriptions.

Example: Display detailed information on a specific drive and library

Display detailed information about the drive named DRIVE02 that is associated with the library LIB2. Issue the command:

```
query drive lib2 drive02 format=detailed
```

```
                               Library Name: LIB2
                                 Drive Name: DRIVE02
                                Device Type: 3590
                                    On-Line: Yes
                                Drive State: Empty
                               Allocated to:
                Last Update by (administrator): ADMIN
                     Last Update Date/Time: 02/29/2002 09:26:23
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE
```

See Field descriptions for field descriptions.

Field descriptions

Library Name
: The name of the library to which the drive is assigned.

Drive Name
: The name assigned to the drive.

Device Type
: The device type as specified in the associated device class. The server must have a path defined from the server to the drive in order to determine the true device type. As long as there is a path defined from the server to the drive, the server will display the true device type of the drive even if there are other paths defined to this drive. Exceptions to this occur if the device type is remote or unknown.

  REMOTE
  : The server does not have a path to the device. The only defined paths to the device are from data movers.

  UNKNOWN
  : No path exists.

  Tip: Review the output of the QUERY PATH command to determine if the desired paths are defined. If they are not defined, define those desired paths using the DEFINE PATH command. Also, if using a data mover device, review the output of the QUERY DATAMOVER command to determine the type of the data mover device. If you are using a path from the server to a drive, the device type of the device class and the drive need to match. If you are using a path from a data mover device to a drive, review the documentation for your type of data mover to ensure the device type of the device class is compatible with the type of data mover device.

On-Line
: Specifies the status of the drive:

  Yes
  : The drive is online and available for server operations.

  No
  : The drive is offline and was put in this state by an administrator updating the status.

  Unavailable Since

Specifies that the drive has been unavailable since *mm/dd/yy hh:mm:ss*. Output shows the time the server marked the drive as unavailable.

Polling Since
Specifies that the server is polling the drive because the drive stopped responding. Output shows the time the server detected a problem and began polling. The server polls a drive before stating it is unavailable. The time output follows the format: mm/dd/yy hh:mm:ss.

Read Formats
The read formats for the drive.

Write Formats
The write formats for the drive.

Element
The element number for the drive.

Drive State
This specifies the current state of this particular drive based on the result of the last SCSI command to the drive or library. The server tracks the state of the drive to improve its selection of a drive for an operation and its drive recovery operations. The values are:

Unavailable
The drive is not available to the library for operations.

Empty
The drive is empty and ready for operations.

Loaded
The drive is currently loaded, and the server is performing operations to the drive.

Unloaded
The media has been ejected from the drive.

Reserved
The drive is reserved for a mount request.

Unknown
The drive begins in drive state unknown as a result of being defined, as a result of server initialization, or as a result of having its status updated to online.

Volume Name
The volume name for the drive.

Allocated To
The name of the library client that is currently using the drive. This applies to shared SCSI libraries only; the field is left blank for all other libraries.

WWN
The World Wide Name for the drive.

Last Update by (administrator)
Who performed the last update to the drive.

Last Update Date/Time
The date and time when the last update occurred.

Cleaning Frequency (Gigabytes/ASNEEDED/NONE)
How often the server activates drive cleaning. This value can be the number of gigabytes, ASNEEDED, or NONE.

Related commands

Table 1. Commands related to QUERY DRIVE

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DRIVE	Deletes a drive from a library.
DELETE LIBRARY	Deletes a library.
QUERY LIBRARY	Displays information about one or more libraries.
UPDATE DRIVE	Changes the attributes of a drive.

QUERY DRMEDIA (Query disaster recovery media)

Use this command to display information about database backup volumes, and volumes in copy storage pools, container-copy storage pools, and active-data storage pools. You can also use the command to create a file of executable commands to process the volumes.

The processing of volumes by this command depends on what the volumes are used for:

Backups of the server database
: To control whether the command processes database backup volumes, use the SOURCE parameter. The command can process volumes that are used for full plus incremental or snapshot database backups. You cannot specify virtual volumes (backup objects that are stored on another server). You can change volumes through each state, or you can use the TOSTATE parameter and skip states to simplify the movements.

Copy storage pools
: The QUERY DRMEDIA command always processes eligible copy storage-pool volumes.

Container-copy storage pools
: By default, volumes in container-copy storage pools are not eligible for processing by the QUERY DRMEDIA command. To process container-copy storage pool volumes, you must issue the SET DRMCOPYCONTAINERSTGPOOL command first, or specify the COPYCONTAINERSTGPOOL parameter on the QUERY DRMEDIA command.

Active-data storage pools
: By default, volumes in active-data storage pools are not eligible for processing by the QUERY DRMEDIA command. To process active-data pool volumes, you must issue the SET DRMACTIVEDATASTGPOOL command first, or specify the ACTIVEDATASTGPOOL parameter on the QUERY DRMEDIA command.

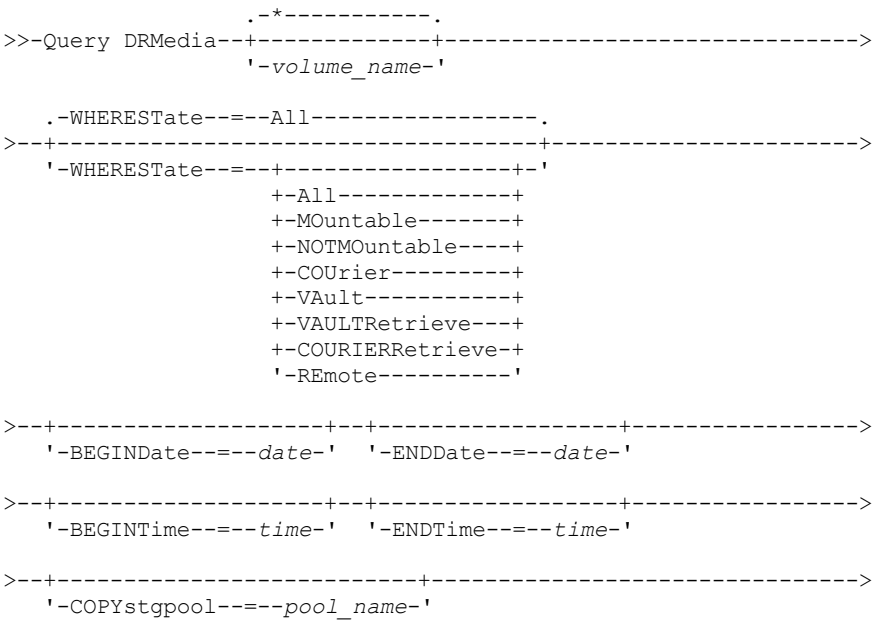
If you are using an external library and have moved a volume to the NOTMOUNTBLE state using the MOVE DRMEDIA command, the QUERY DRMEDIA command might still report the volume state as MOUNTABLE if it detects that the volume is in the library. Refer to the external library documentation for information about the procedures that you should follow when you use the MOVE DRMEDIA and the QUERY DRMEDIA commands.

Privilege class

To issue this command, you must have one of the following privilege classes:

- *If the CMD parameter is NOT specified:* operator or system privilege.
- *If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO:* operator, unrestricted storage, or system privilege.
- *If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES (the default):* system privilege.

Syntax



Parameters

volume_name
: Specifies the names of the volumes to be queried. You can use wildcard characters to specify multiple names. This parameter is optional. The server looks for matching names among the following eligible volumes:

  - Database backup volumes, as selected by the SOURCE parameter of this command.
  - Copy storage pool volumes from copy storage pools specified by the COPYSTGPOOL parameter. If you do not use the COPYSTGPOOL parameter, the server queries volumes from copy storage pools previously specified by the SET DRMCOPYSTGPOOL command.
  - Active-data storage pool volumes from active-data storage pools specified by the ACTIVEDATASTGPOOL parameter. If you do not use the ACTIVEDATASTGPOOL parameter, the server queries volumes from active-data storage pools that were previously specified by the SET DRMACTIVEDATASTGPOOL command.
  - Container-copy storage pool volumes from container-copy storage pools specified by the COPYCONTAINERSTGPOOL parameter. If you do not use the COPYCONTAINERSTGPOOL parameter, the server queries volumes from container-copy storage pools that were previously specified by the SET DRMCOPYCONTAINERSTGPOOL command.

  Other parameters can also limit the results of the query.

WHERE State
: Specifies the state of volumes to be processed. This parameter is optional. The default is ALL. Possible values are:

  All
  : Specifies all volumes in all states.

  MOuntable
  : Volumes in this state contain valid data and are accessible for onsite processing.

  NOTMOuntable
  : Volumes in this state are onsite, contain valid data, and not accessible for onsite processing.

  COUrier
  : Volumes in this state are being moved to an offsite location.

  VAult
  : Volumes in this state are offsite, contain valid data, and are not accessible for onsite processing.

  VAULTRetrieve
  : Volumes in this state are located at the offsite vault, do not contain valid data, and can be moved back onsite for reuse or disposal:

    - A copy storage pool volume is considered to be in the VAULTRETRIEVE state if it has been empty for at least the number of days specified with the REUSEDELAY parameter on the DEFINE STGPOOL command.
    - A database backup volume is considered to be in the VAULTRETRIEVE state if it is associated with a database backup series that was expired based on the value specified using the SET DRMDBBACKUPEXPIREDAYS command.

    Important: When you issue QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE, the server dynamically determines which volumes can be moved back onsite for reuse or disposal. Therefore, to ensure that you identify all volumes that are in a VAULTRETRIEVE state, issue QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE without the BEGINDATE,

ENDDATE, BEGINTIME or ENDTIME parameters. The `Last Update Date/Time` field in the output for QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE displays the date and time that a volume was moved to the VAULT state, not VAULTRETRIEVE.

COURIERRetrieve
: Volumes in this state are being moved back to the onsite location.

REmote
: Volumes in this state contain valid data and are located at the offsite remote server.

BEGINDate
: Specifies the beginning date used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command has changed the volume to its current state on or after the specified date. The default is the earliest date for which volume information exists.
You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified. The maximum number of days is 9999.	TODAY-7 *or* -7. To query volumes beginning with records changed to their current state a week ago, you can specify BEGINDATE=TODAY-7 or BEGINDATE=-7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDDate
: Specifies the ending date used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command has changed the volume to its current state on or before the specified date. The default is the current date.
You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified. The maximum number of days is 9999.	TODAY-7 *or* -7. To query volumes beginning with records changed to their current state a week ago, you can specify BEGINDATE=TODAY-7 or BEGINDATE=-7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command has changed the volume to its current state on or after the specified time and date. The default is midnight (00:00:00) on the date specified with the BEGINDATE parameter.

You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	12:33:28
NOW	The current time on the specified begin date	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 *or* +03:00. If you issue QUERY DRMEDIA command at 9:00 with BEGINTIME=NOW+03:00 or BEGINTIME=+03:00. The server displays volumes that were changed to their current state at 12:00 on the begin date that you specify.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-03:30 *or* -03:30. If you issue QUERY DRMEDIA command at 9:00 with BEGINTIME=NOW-03:30 or BEGINTIME=-03:30. The server displays volumes that were changed to their current state at 5:30 on the begin date that you specify.

ENDTime

Specifies the ending time used to select volumes. This parameter is optional. Volumes are considered eligible if the MOVE DRMEDIA command has changed the volume to its current state on or before the specified time and date. The default is 23:59:59.

You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 *or* +03:00. If you issue QUERY DRMEDIA command at 9:00 with ENDTIME=NOW+03:00 or ENDTIME=+03:00, IBM Spectrum Protect™ processes volumes that were changed to their current state at 12:00 on the end date you specify.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date	NOW-03:30 *or* -03:30 If you issue QUERY DRMEDIA command at 9:00 with ENDTIME=NOW-03:00 or ENDTIME=-03:00, IBM Spectrum Protect processes volumes that were changed to their current state at 6:00 on the end date you specify.

COPYstgpool

Specifies the name of the copy storage pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. The copy storage pools specified with this parameter override those specified with the SET DRMCOPYSTGPOOL command.

If this parameter is not specified, the server selects the storage pools as follows:

- If the SET DRMCOPYSTGPOOL command was previously issued with valid copy storage pool names, the server processes only those storage pools.
- If the SET DRMCOPYSTGPOOL command has not been issued, or if all of the copy storage pools have been removed using the SET DRMCOPYSTGPOOL command, the server processes all copy storage pool volumes in the specified state (ALL, MOUNTABLE, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE, or REMOTE).

Source
Specifies whether any database backup volumes are selected. This parameter is optional. The default is DBBACKUP. Possible values are:

DBBackup
Full and incremental database backup volumes are selected.
DBSnapshot
Snapshot database backup volumes are selected.
DBNone
No database backup volumes are selected.

ACTIVEDatastgpool
Specifies the name of the active-data storage pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. The active-data storage pools that are specified with this parameter override those specified with the SET DRMACTIVEDATASTGPOOL command.

If this parameter is not specified, the server selects the storage pools as follows:

- If the SET DRMACTIVEDATASTGPOOL command was previously issued with valid active-data storage pool names, the server processes only those storage pools.
- If the SET DRMACTIVEDATASTGPOOL command has not been issued, or all of the active-data storage pools have been removed using the SET DRMACTIVEDATASTGPOOL command, the server processes all active-data storage pool volumes in the specified state (ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE, or REMOTE). Volumes in the MOUNTABLE state are not processed.

COPYCONtainerstgpool
Specifies the name of the container-copy storage pool whose volumes are to be processed. This parameter is optional. You can use wildcard characters to specify this name. The container-copy storage pools that are specified using this parameter override those that are specified using the SET DRMCOPYCONTAINERSTGPOOL command.

If this parameter is not specified, the server selects the storage pools as follows:

- If the SET DRMCOPYCONTAINERSTGPOOL command was previously issued with names of valid container-copy storage pools, the server processes only those storage pools.
- If the SET DRMCOPYCONTAINERSTGPOOL command has not been issued, or if all container-copy storage pools were removed using the SET DRMCOPYCONTAINERSTGPOOL command, the server processes all container-copy pool volumes based on the value that is specified by the WHERESTATE parameter. If the parameter is set to a value of ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE, or REMOTE, the volumes are processed. If the value is set to MOUNTABLE, the volumes are not processed.

Format
Specifies the information to be displayed. This parameter is optional. The default is STANDARD. Possible values are:

Standard
Specifies that partial information is displayed.
Detailed
Specifies that detailed information is displayed.
Cmd
Specifies that executable commands are built for the selected volumes. If you specify FORMAT=CMD, you must also specify the CMD parameter.

WHERELOcation

Specifies the location of the volumes to be queried. This parameter is optional. The maximum length of the location is 255 characters. Enclose the text in quotation marks if it contains any blank characters. If you specify a target server name, the disaster recovery manager displays all database backup volumes and copy storage pool volumes located on the target server.

CMd

Specifies the creation of executable commands to process the volume name and location obtained by this command. This parameter is optional. You must enclose the command specification in quotation marks. The maximum length of this parameter is 255 characters. The disaster recovery manager writes the commands to a file specified by the CMDFILENAME parameter or the SET DRMCMDFILENAME command, or generated by the QUERY DRMEDIA command. If the command length is greater than 240 characters, it is split into multiple lines and continuation characters (+) are added. You may need to alter the continuation character according to the product that runs the commands.

If you do not specify the FORMAT=CMD parameter, this command will not create any command lines.

string

The command string. The string must not include embedded quotation marks. For example, this is a valid CMD parameter:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

This is an example of a CMD parameter that is *not* valid:

```
cmd=""checkin libvolume lib8mm" &vol status=scratch""
```

substitution

Specifies a substitution variable to tell QUERY DRMEDIA to substitute a value for the variable. The variables are not case-sensitive, and must not contain blank spaces after the ampersand (&). The possible variables are:

&VOL

A volume name variable.

&LOC

A volume location.

&VOLDSN

The name of the file the server writes into the sequential access media labels. An example of a copy storage pool tape volume file name using the default prefix TSM is TSM.BFS. An example of a database backup tape volume file name using a prefix TSM310 defined with the device class is TSM310.DBB.

&NL

The new line character. When &NL is specified, QUERY DRMEDIA command splits the command at the &NL variable and does not append a continuation character. You must specify the proper continuation character before the &NL if one is required. If the &NL is not specified and the command line is greater than 240 characters, the line is split into multiple lines and continuation characters (+) are added.

AIX | Linux CMDFilename

AIX | Linux Specifies the fully qualified name of the file to contain the commands specified with CMD parameter. This parameter is optional.

If you do not specify a name with the SET DRMCMDFILENAME command, the server creates a file name by appending `exec.cmds` to the absolute directory path name of the IBM Spectrum Protect instance directory. If you specify a null string (" "), the commands are displayed on the console only. You can redirect the commands to a file using the redirection character for the operating system.

If the operation fails after the command file is created, the file is not deleted.

Windows CMDFilename

Windows Specifies the fully qualified name of the file to contain the commands specified with CMD parameter. This parameter is optional.

If you do not specify a file name with the SET DRMCMDFILENAME command, the server creates a file name by appending `exec.cmd` to the directory that represents this instance of the server (typically the directory where the IBM Spectrum Protect server was originally installed). If you specify a null string (""), the commands are displayed on the console only. You can redirect the commands to a file by using > or >> provided by the system. The disaster recovery manager allocates the file name specified or generated. If the file exists, the disaster recovery manager tries to use it and any existing data is overwritten.

If the operation fails after the command file is created, the file is not deleted.

APPend
: Specifies whether to overwrite any existing contents of the command file or append the commands to the file. This parameter is optional. The default is NO. Possible values are:

  No
  : The disaster recovery manager overwrites the contents of the file.

  Yes
  : The disaster recovery manager appends the commands to the file.

Example: List volumes to be sent to offsite storage

Display all volumes to be given to a courier for offsite storage.

```
query drmedia wherestate=notmountable
format=standard

Volume Name      State           Last Update           Automated
                                 Date/Time             LibName
---------------  --------------  --------------------  ---------
TAPE01           Not mountable    01/20/1998 14:25:22
DBTP01           Not mountable    01/20/1998 14:25:22
DBTP03           Not mountable    01/20/1998 14:31:53
```

See Field descriptions for field descriptions.

Example: Display information on volumes at the vault

Display detailed information about all volumes at the vault.

```
query drmedia wherestate=vault format=detailed

                     Volume Name: DBTP02
                           State: Vault
           Last Update Date/Time: 01/20/1998 13:29:02
                        Location: Ironmnt
                     Volume Type: DBBackup
          Copy Storage Pool Name:
   Active-Data Storage Pool Name: TSMACTIVEPOOL
               Automated LibName:
```

See Field descriptions for field descriptions.

Field descriptions

Volume Name
: The name of the database backup or copy storage pool volume.

State
: The state of the volume.

Last Update Date/Time
: The date and time that the volume state was last updated. For volumes in the VAULTRETRIEVE state, this field displays the date and time that a volume was moved to the VAULT state, not VAULTRETRIEVE. The server does not "update" volumes to VAULTRETRIEVE. At the time the QUERY DRMEDIA command is issued, the server dynamically determines whether the data in copy storage pool volumes and database backup volumes is no longer valid and whether the volume can be brought back onsite for reuse or disposal.

Location
: The Location field is displayed when the volume is not mountable or when it's not in the library. The Location field is empty if the volume is mountable and is in the library.

Volume Type
: The type of volume. Possible values are:

  DBBackup
  : A full or incremental database backup volume.

  DBSnapshot
  : A database snapshot backup volume.

  CopyStgPool
  : A copy storage pool volume.

ContcopyStgPool
A container-copy storage pool volume.

Copy Storage Pool Name
For a copy storage pool volume, the name of the copy storage pool.
Active Data Storage Pool Name
For an active-data storage pool volume, the name of the active-data storage pool.
Container-Copy Storage Pool Name
For a container-copy storage pool volume, the name of the container-copy storage pool.
Automated LibName
The name of the automated library if the volume is in a library.

Related commands

Table 1. Commands related to QUERY DRMEDIA

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMSTATUS	Displays DRM system parameters.
SET DRMACTIVEDATASTGPOOL	Specifies that active-data storage pools are managed by DRM.
AIX Linux Windows SET DRMCOPYCONTAINERSTGPOOL	Specifies the container-copy storage pools that are used in DRM commands.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.
SET DRMCMDFILENAME	Specifies a file name for containing DRM executable commands.
SET DRMFILEPROCESS	Specifies whether the MOVE DRMEDIA or QUERY DRMEDIA command processes files associated with a device type of file.

QUERY DRMSTATUS (Query disaster recovery manager system parameters)

Use this command to display information about the system parameters defined for disaster recovery manager (DRM).

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query DRMSTatus-------------------------------------------><
```

Parameters

None.

Example: Display DRM system parameter information

Display information about the DRM system parameters:

```
query drmstatus

              Recovery Plan Prefix:
         Plan Instructions Prefix:
       Replacement Volume Postfix: @
            Primary Storage Pools: PRIM1 PRIM2
               Copy Storage Pools: COPY*
        Active-Data Storage Pools: TSMACTIVEPOOL
     Container-Copy Storage Pools: COPYCNTRPOOL
      Not Mountable Location name: Local
                     Courier Name: Fedex
                  Vault Site Name: Ironmnt
  DB Backup Series expiration days: 30 Day(s)
Recovery Plan File Expiration Days: 30 Days(s)
                     Check Label?: No
         Process FILE Device Type?: No
                  Command file name:
```

Field descriptions

Recovery Plan Prefix
: User-specified prefix portion of the file name for the recovery plan file.

Plan Instructions Prefix
: User-specified prefix portion of the file names for the server recovery instructions files.

Replacement Volume Postfix
: The character added to the end of the replacement volume names in the recovery plan file.

Primary Storage Pools
: The primary storage pools that are eligible for processing by the PREPARE command. If this field is blank, all primary storage pools are eligible.

Copy Storage Pools
: The copy storage pools that are eligible for processing by the MOVE DRMEDIA, PREPARE, and QUERY DRMEDIA commands. If this field is blank, all copy storage pools are eligible.

Active-Data Storage Pools
: The active-data pools that are eligible for processing by the MOVE DRMEDIA, PREPARE, and QUERY DRMEDIA commands. If this field is blank, active-data pools are not eligible.

Container-Copy Storage Pools
: The container-copy storage pools that are eligible for processing by the MOVE DRMEDIA, PREPARE, and QUERY DRMEDIA commands. If this field is blank, container-copy storage pools are not eligible.

Not Mountable Location Name
: The name of the offsite location where the media to be shipped are stored.

Courier Name
: The name of the courier used to carry the media to the vault.

Vault Site Name
: The name of the vault where the media is stored.

DB Backup Series Expiration Days
: The minimum number of days that must elapse since a database series has been created before it is eligible to be expired. See the SET DRMDBBACKUPEXPIREDAYS command for information about the criteria that must be met for database backup series expiration.

Recovery Plan File Expiration Days
: The minimum number of days that must elapse since a recovery plan file, stored on a target server, has been created before it is eligible to be expired. See the SET DRMRPFEXPIREDAYS command for information about the criteria that must be met for recovery plan file expiration.

Check Label?
: Whether media labels are read for sequential media volumes checked out by the MOVE DRMEDIA command. Possible values are Yes or No.

Process FILE Device Type?
: Whether MOVE DRMEDIA or QUERY DRMEDIA commands process database backup and copy storage pool volumes associated with a device class with a FILE device type. Possible values are Yes or No.

Command File Name
: The full path file name that contains the executable commands generated by the MOVE DRMEDIA or QUERY DRMEDIA command.

Related commands

Table 1. Commands related to QUERY DRMSTATUS

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
PREPARE	Creates a recovery plan file.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
SET DRMCHECKLABEL	Specifies whether IBM Spectrum Protect should read volume labels during MOVE DRMEDIA command processing.
SET DRMACTIVEDATASTGPOOL	Specifies that active-data storage pools are managed by DRM.
AIX Linux Windows SET DRMCOPYCONTAINERSTGPOOL	Specifies the container-copy storage pools that are used in DRM commands.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.
SET DRMCMDFILENAME	Specifies a file name for containing DRM executable commands.
SET DRMCOURIERNAME	Specifies the name of the courier for the disaster recovery media.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.
SET DRMFILEPROCESS	Specifies whether the MOVE DRMEDIA or QUERY DRMEDIA command processes files associated with a device type of file.
SET DRMINSTRPREFIX	Specifies the prefix portion of the path name for the recovery plan instructions.
SET DRMPLANVPOSTFIX	Specifies the replacement volume names in the recovery plan file.
SET DRMPLANPREFIX	Specifies the prefix portion of the path name for the recovery plan.
SET DRMPRIMSTGPOOL	Specifies that primary storage pools are managed by DRM.
SET DRMRPFEXPIREDAYS	Set criteria for recovery plan file expiration.
SET DRMVAULTNAME	Specifies the name of the vault where DRM media is stored.
SET DRMNOTMOUNTABLENAME	Specifies the location name of the DRM media to be sent offsite.

QUERY ENABLED (Query enabled events)

Use this command to display either a list of enabled events or a list of disabled events, whichever is shorter.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query--ENabled--+-CONSOLE--------+-------------------------->
                   +-ACTLOG---------+
                   +-EVENTSERVER----+
                   +-FILE-----------+
                   +-FILETEXT-------+
                   |            (1) |
                   +-NTEVENTLOG-----+
                   |        (2)     |
                   +-SYSLOG---------+
                   +-TIVOLI---------+
                   '-USEREXIT-------'
```

```
>--+---------------------------+-----------------------------><
   +-NODEname--=--node_name-----+
   '-SERVername--=--server_name-'
```

Notes:

1. This parameter is only available for the Windows operating system.
2. This parameter is only available for the Linux operating system.

Parameters

receiver
: Specifies a type of receiver for enabled events. This is a required parameter. Valid values are:

  ACTLOG
  : Specifies the IBM Spectrum Protect™ activity log as a receiver.

  CONSOLE
  : Specifies the standard server console as a receiver.

  EVENTSERVER
  : Specifies the event server as a receiver.

  FILE
  : Specifies a user file as a receiver. Each logged event is a record in the file and a person cannot read each logged event easily.

  FILETEXT
  : Specifies a user file as a receiver. Each logged event is a fixed-size, readable line.

  Windows NTEVENTLOG
  : Windows Specifies the Windows application log as a receiver.

  Linux SYSLOG
  : Linux Specifies the Linux system log as a receiver.

  TIVOLI
  : Specifies the Tivoli Management Environment (TME) as a receiver.

  USEREXIT
  : Specifies a user-written routine to which IBM Spectrum Protect writes information as a receiver.

NODEname
: Specifies a node name to be queried. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the query is for events enabled for the server running this command.

SERVername
: Specifies a server name to be queried. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the query is for events enabled for the server running this command.

Example: Query the server for console events

Query the server for server events that are enabled for the console. There are 10000 possible server events. Either a list of enabled events or disabled events is displayed (whichever list is shorter).

```
query enabled console

9998 events are enabled for the CONSOLE receiver.  The
following events are DISABLED for the CONSOLE receiver:

ANR8409, ANR8410
```

Related commands

Table 1. Commands related to QUERY ENABLED

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DISABLE EVENTS	Disables specific events for receivers.
ENABLE EVENTS	Enables specific events for receivers.
END EVENTLOGGING	Ends event logging to a specified receiver.

Command	Description
QUERY EVENTRULES	Displays information about rules for server and client events.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

QUERY EVENT (Query scheduled and completed events)

Use this command to display the status of scheduled events. The time and date parameters allow you to limit the query to events that were scheduled to occur within the specified times and dates. Limiting the output to events whose scheduled start times fall within a date and time range also minimizes the time it takes to process this query.

The command syntax differs for queries that apply to scheduled client operations and to scheduled administrative commands.

Table 1. Commands related to QUERY EVENT

Command	Description
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
DELETE EVENT	Deletes event records before a specified date and time.
QUERY ACTLOG	Displays messages from the server activity log.
SET EVENTRETENTION	Specifies the number of days to retain records for scheduled operations.
SET RANDOMIZE	Specifies the randomization of start times within a window for schedules in client-polling mode.

- QUERY EVENT (Display client schedules)
  Use the QUERY EVENT command to display scheduled and completed events for selected clients.
- QUERY EVENT (Display administrative event schedules)
  Use the QUERY EVENT command to display scheduled and completed events for selected administrative command schedules.

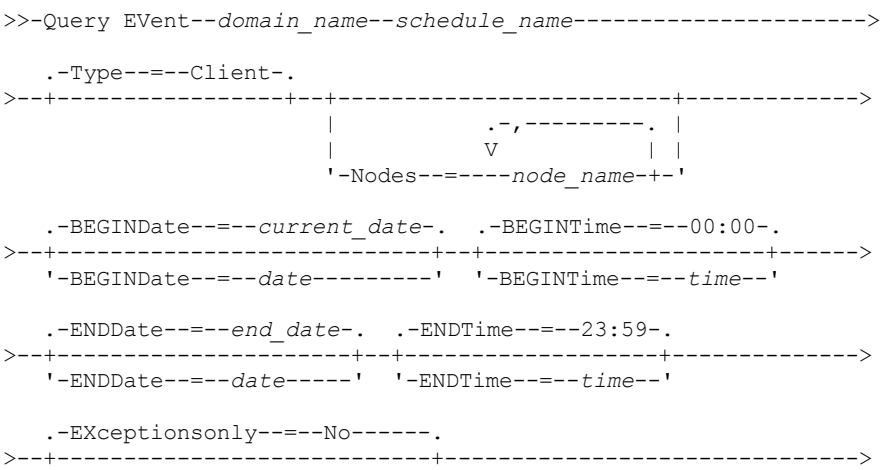
QUERY EVENT (Display client schedules)

Use the QUERY EVENT command to display scheduled and completed events for selected clients.

Privilege class

Any administrator can issue this command.

Syntax



```
   '-EXceptionsonly--=--+-No--+-'
                        '-Yes-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the schedules belong. You can use a wildcard character to specify this name.

schedule_name (Required)
: Specifies the name of the schedule for which events are displayed. You can use a wildcard character to specify this name.

Type=Client
: Specifies that the query displays events for client schedules. This parameter is optional. The default is CLIENT.

Nodes
: Specifies the name of the client node that belongs to the specified policy domain for which events are displayed. You can specify multiple client nodes by separating the names with commas and no intervening spaces. You can use wildcard characters to specify nodes. If you do not specify a client name, events display for all clients that match the domain name and the schedule name.

BEGINDate
: Specifies the beginning date of the time range for events to be displayed. All events scheduled to start during this time are displayed. This parameter is optional. The default is the current date.
You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
TODAY-days **or** -days	The current date minus days specified	TODAY-7 **or** -7. To query events scheduled to start during the past seven days, specify BEGINDATE=TODAY-7 ENDDATE=TODAY or BEGINDATE=-7 ENDDATE=TODAY.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime
: Specifies the beginning time of the range for events to be displayed. All events scheduled to start during this time are displayed. This parameter is optional. The default value is 00:00.
You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	10:30:08

Value	Description	Example
NOW	The current time on the specified begin date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 to query events scheduled to start 3 hours from now, you can specify either BEGINTIME=NOW+03:00 or BEGINTIME=+03:00. IBM Spectrum Protect™ displays events at 12:00 on the specified begin date.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-04:00 **or** -04:00. If you issue this command at 9:00 to query events scheduled to start during the last 4 hours, you can specify either BEGINTIME=NOW-04:00 ENDTIME=NOW or BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect displays events at 5:00 on the specified begin date.

ENDDate

Specifies the ending date of the time range for events to be displayed. All events that were schedule to start during this time are displayed. This parameter is optional. The default is the value used for the BEGINDATE.
You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
TODAY-days **or** -days	The current date minus days specified	TODAY-8 **or** -8. To query events scheduled to start during a one-week period that ended yesterday, you can specify either BEGINDATE=TODAY-8 ENDDATE=TODAY-1 or BEGINDATE=-8 ENDDATE=-1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time of the range for events to be displayed. All events that were scheduled to start during this time are displayed. This parameter is optional. The default value is 23:59.
You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW

Value	Description	Example
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 to query events scheduled to start 3 hours from now, you can specify either BEGINTIME=NOW ENDTIME=NOW+03:00 or BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified end date	NOW-04:00 **or** -04:00

EXceptionsonly
: Specifies the type of information you want on scheduled or completed events. This parameter is optional. The default is NO. You can specify one of the following values:

  No
  : Specifies that the information on past and projected events is displayed.

  Yes
  : Specifies that the events that failed or did not process as scheduled are displayed.

Format
: Specifies how information displays. This parameter is optional. The default is STANDARD. The following values are possible:

  Standard
  : Specifies that partial information for events displays.

  Detailed
  : Specifies that complete information for events displays.

Display partial information for unsuccessful events

Display partial information for all events that are scheduled for DOMAIN1 that did not run successfully. Limit the search to the client named JOE. Limit the events that are displayed to events that were scheduled to occur from February 11, 2001 (02/11/2001) to February 12, 2001 (02/12/2001).

```
query event domain1 * nodes=joe begindate=02/11/2001
enddate=02/12/2001 exceptionsonly=yes

Scheduled Start      Actual Start          Schedule  Node    Status
                                            Name     Name
-------------------- --------------------  --------- ----   ---------
02/11/1999 01:00:00  02/11/1999 01:13:55   BACK1      JOE   Failed
02/12/1999 01:00:00                        DAILYBKP   JOE   Missed
```

See Field descriptions for field descriptions.

Display partial information for scheduled events for a client

Display complete information for all events that are scheduled for processing. Use the start time as 10 days previous to today, and the finish includes today.

```
query event * * begindate=today-10 enddate=today

Scheduled Start         Actual Start            Schedule Name    Node Name        Status
-------------------     --------------------    -------------    -------------    ---------
02/04/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/04/2013 14:00:00     02/04/2013 14:12:49     VDATAMVR1-IN1    VDATAMVR1-T1     Completed
02/04/2013 14:30:00     02/04/2013 14:33:10     VDATAMVR1-IN2    VDATAMVR1-T2     Completed
02/04/2013 15:00:00     02/04/2013 15:01:49     VDATAMVR1-IN3    VDATAMVR1-T3     Completed
02/04/2013 15:30:00     02/04/2013 15:42:00     VDATAMVR1-IN4    VDATAMVR1-T4     Completed
02/05/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/05/2013 14:00:00     02/05/2013 14:05:22     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/05/2013 14:30:00     02/05/2013 14:32:53     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/05/2013 15:00:00     02/05/2013 15:00:38     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/05/2013 15:30:00     02/05/2013 15:36:41     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/06/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/06/2013 14:00:00     02/06/2013 14:06:42     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/06/2013 14:30:00     02/06/2013 14:35:41     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/06/2013 15:00:00     02/06/2013 15:08:56     VDATAMVR1-F3     VDATAMVR1-F3     Completed
```

```
02/06/2013 15:30:00     02/06/2013 15:40:49     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/07/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/07/2013 14:00:00     02/07/2013 14:03:43     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/07/2013 14:30:00     02/07/2013 14:35:10     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/07/2013 15:00:00     02/07/2013 15:09:12     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/07/2013 15:30:00     02/07/2013 15:40:21     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/08/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/08/2013 14:00:00     02/08/2013 14:10:17     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/08/2013 14:30:00     02/08/2013 14:39:16     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/08/2013 15:00:00     02/08/2013 15:08:17     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/08/2013 15:30:00     02/08/2013 15:41:16     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/09/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/09/2013 14:02:16                             VDATAMVR1-F1     VDATAMVR1-F1     Failed 12
02/09/2013 14:30:00     02/09/2013 14:44:26     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/09/2013 15:00:00     02/09/2013 15:06:24     VDATAMVR1-F3     VDATAMVR1-F3     Failed 12
02/09/2013 15:30:00     02/09/2013 15:32:18     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/11/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/11/2013 14:00:00     02/11/2013 14:01:05     VDATAMVR1-F1     VDATAMVR1-F1     Failed 12
02/11/2013 14:30:00     02/11/2013 14:31:42     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/11/2013 15:00:00     02/11/2013 15:06:17     VDATAMVR1-F3     VDATAMVR1-F3     Failed 12
02/11/2013 15:30:00     02/11/2013 15:30:19     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/12/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/12/2013 14:00:00     02/12/2013 14:03:37     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/12/2013 14:30:00     02/12/2013 14:33:07     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/12/2013 15:00:00     02/12/2013 15:03:56     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/12/2013 15:30:00     02/12/2013 15:36:44     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/13/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/13/2013 14:00:00     02/13/2013 14:06:24     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/13/2013 14:30:00     02/13/2013 14:34:50     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/13/2013 15:00:00     02/13/2013 15:15:01     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/13/2013 15:30:00     02/13/2013 15:30:18     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/14/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Future
02/14/2013 14:00:00                             VDATAMVR1-F1     VDATAMVR1-F1     Future
02/14/2013 14:30:00                             VDATAMVR1-F2     VDATAMVR1-F2     Future
02/14/2013 15:00:00                             VDATAMVR1-F3     VDATAMVR1-F3     Future
```

See Field descriptions for field descriptions.

Display detailed information for scheduled events for a client

Display the detailed information for events that are scheduled for processing by client DOC between the hours of 10:00 AM and 11:00 AM on November 1, 2005 (11/01/2005). Notice that when the status is FAILED, the result code is displayed.

```
query event domain1 * nodes=doc begindate=11/01/2005
begintime=10:00 endtime=11:00 enddate=11/01/2005
exceptionsonly=yes format=detailed
```

```
Scheduled Start      Actual Start         Schedule   Node    Status
                                          Name       Name
-------------------- -------------------- ---------  ------  -------
11/01/2005 10:01:01  11/01/2005 10:03:46  T1         DOC     Failed 8
11/01/2005 10:16:01  11/01/2005 10:16:10  T1         DOC     Failed 4
11/01/2005 10:31:01  11/01/2005 10:33:08  T1         DOC     Completed
11/01/2005 10:46:01                       T1         DOC     Missed
11/01/2005 10:57:49  11/01/2005 10:58:07  T0         DOC     Failed 12
```

Field descriptions

Policy Domain Name
: Specifies the name of the policy domain to which the schedule is assigned.

Schedule Name
: Specifies the name of the schedule that initiated this event.

Node Name
: Specifies the client that is scheduled to perform the operation.

Scheduled Start
: Specifies the scheduled starting date and time for the event.

Actual Start
: Specifies the date and time at which the client began processing the scheduled operation. No information is displayed if the scheduled operation has not started.

Completed

Specifies the date and time the scheduled event is completed.

Status

Specifies the status of the event at the time the QUERY EVENT command is issued. The following values are possible:

Completed
: Specifies that the scheduled event is completed.

Failed
: Specifies that the client reports a failure when you run the scheduled operation and successive retries failed.

Failed - no restart
: Specifies an intermediate status, when a client session is interrupted by a communications error or timeout on the server. This status can be changed to a final status of "Completed" or "Failed" when the event completes.

Future
: Specifies that the beginning of the startup window for the event is in the future. This status also indicates that an event record has not been created for this event.

In Progress
: Specifies that the scheduled event is running and has not yet reported the completion state to the server.

  Periodically check the status for completion of the scheduled event. If this status is not updated in a reasonable amount of time, review your client dsmsched.log and dsmerror.log to determine why the client did not report the outcome of this event to the server. If the scheduled backup failed, rerun the scheduled event or perform a manual incremental backup to ensure the data backup.

Missed
: Specifies that the scheduled startup window for this event passed and the schedule did not begin.

Pending
: Specifies that the QUERY EVENT command was issued during the startup window for the event, but processing the scheduled operation did not begin.

Restarted
: Specifies that the client has tried to process the scheduled operation again.

Severed
: Specifies that the communications with the client is severed before the event can complete.

Started
: Specifies that the event has begun processing.

Uncertain
: Specifies that the state of the event cannot be determined. The server specifies `Uncertain` if the QUERY EVENT command does not find an event record. An event record is not found if the record was deleted or if the server was unavailable during the scheduled startup window (the schedule was never started). Records with Uncertain status are not stored in the database. If you do not want these records to display, either specify EXCEPTIONSONLY=YES or delete the schedule if it is no longer needed.

Attention: When a scheduled operation is processing, and is not restarted within its specified duration, the Status field shows `Started`. If the operation continues beyond the specified duration, no event record is created. If a query is issued after the specified duration has passed, the Status shows as `Failed` even if the operation is still running. After the operation completes, an event record is created, and a subsequent query shows the result in the Status field.

Result

Specifies the return code that indicates whether the schedule processed successfully. If the return code is a value other than 0, examine the server activity log and the client's error log and schedule log.

Return code	Explanation
0	All operations were completed successfully.
4	The operation was completed, but some files were not processed.
8	The operation was completed with at least one warning message.
12	The operation was completed with at least one error message. The count of error messages does not include notifications about skipped files.
-99	The operation failed because the session between the client and the server ended for an unknown reason. It is unknown whether the client can reconnect to the server to complete the schedule event.

If a schedule has ACTION=COMMAND as a parameter, and the command is not an IBM Spectrum Protect command, the command can produce other values in the Result field.

Reason
: Specifies the reason for the return code.

QUERY EVENT (Display administrative event schedules)

Use the QUERY EVENT command to display scheduled and completed events for selected administrative command schedules.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query EVent--schedule_name--Type--=--Administrative---------->

   .-BEGINDate--=--current_date-.  .-BEGINTime--=--00:00-.
>--+----------------------------+--+--------------------+------>
   '-BEGINDate--=--date---------'  '-BEGINTime--=--time--'

   .-ENDDate--=--begin_date-.  .-ENDTime--=--23:59-.
>--+-----------------------+--+------------------+------------>
   '-ENDDate--=--date-------'  '-ENDTime--=--time--'

   .-EXceptionsonly--=--No------.
>--+-----------------------------+------------------------------>
   '-EXceptionsonly--=--+-No--+-'
                        '-Yes-'

   .-Format--=--Standard-----.
>--+-------------------------+-------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

schedule_name (Required)
: Specifies the name of the schedule for which events display. You can use wildcard characters to specify names.

Type=Administrative (Required)
: Specifies that the query displays events for administrative command schedules.

BEGINDate
: Specifies the beginning date of the time range for events to be displayed. All events scheduled to start during this time are displayed. This parameter is optional. The default is the current date.

You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
TODAY-days **or** -days	The current date minus days specified	TODAY-7 **or** -7. To query events scheduled to start during the past seven days, specify BEGINDATE=TODAY-7 ENDDATE=TODAY or BEGINDATE=-7 ENDDATE=TODAY.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM

Value	Description	Example
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time of the range for events to be displayed. All events scheduled to start during this time are displayed. This parameter is optional. The default value is 00:00.
You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	10:30:08
NOW	The current time on the specified begin date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 to query events scheduled to start 3 hours from now, you can specify either BEGINTIME=NOW+03:00 or BEGINTIME=+03:00. IBM Spectrum Protect™ displays events at 12:00 on the specified begin date.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-04:00 **or** -04:00. If you issue this command at 9:00 to query events scheduled to start during the last 4 hours, you can specify either BEGINTIME=NOW-04:00 ENDTIME=NOW or BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect displays events at 5:00 on the specified begin date.

ENDDate

Specifies the ending date of the time range for events to be displayed. All events that were schedule to start during this time are displayed. This parameter is optional. The default is the value used for the BEGINDATE.
You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
TODAY-days **or** -days	The current date minus days specified	TODAY-8 **or** -8. To query events scheduled to start during a one-week period that ended yesterday, you can specify either BEGINDATE=TODAY-8 ENDDATE=TODAY-1 or BEGINDATE=-8 ENDDATE=-1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM

Value	Description	Example
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time of the range for events to be displayed. All events that were scheduled to start during this time are displayed. This parameter is optional. The default value is 23:59.
You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 to query events scheduled to start 3 hours from now, you can specify either BEGINTIME=NOW ENDTIME=NOW+03:00 or BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified end date	NOW-04:00 **or** -04:00

EXceptionsonly

Specifies the type of information you want on scheduled or completed events. This parameter is optional. The default is NO. You can specify one of the following values:

No
: Specifies that the information on past and projected events is displayed.

Yes
: Specifies that the events that failed or did not process as scheduled are displayed.

Format

Specifies how the information displays. This parameter is optional. The default value is STANDARD. Possible values are:

Standard
: Specifies that partial information for events displays.

Detailed
: Specifies that complete information for events displays.

Example: List events for a specific administrative schedule

Display partial information for all events scheduled for an administrative schedule named DOSADMIN. Limit the query to events that are scheduled for March 30, 1999 (03/30/1999). Issue the command:

```
query event dosadmin type=administrative
begindate=03/30/1999
enddate=03/30/1999

Scheduled Start      Actual Start          Schedule Status
                                           Name
-------------------- --------------------  --------- ---------
03/30/1999 00:00:00  03/30/1999 00:00:01   DOSADMIN  Completed
03/30/1999 04:00:00  03/30/1999 04:00:01   DOSADMIN  Completed
03/30/1999 12:00:00                        DOSADMIN  Future
03/30/1999 16:00:00                        DOSADMIN  Future
```

Field descriptions

Scheduled Start
: Specifies the scheduled starting date and time for the event.

Actual Start
: Specifies the date and time at which the client began processing the scheduled operation. No information displays if the schedule has not started executing.

Schedule Name
: Specifies the name of the schedule that initiated this event.

Status
: For administrative commands or scripts that specify WAIT=YES, the status of a scheduled event is STARTED until the operation specified by the command or script is completed. The final status of the scheduled event depends on the return code of the operation. However, if WAIT=YES and if the schedule is running a script that specifies PREVIEW=YES, the final status is COMPLETED, unless the script contained a syntax error.

  For administrative commands or scripts that specify WAIT=NO, the status of a scheduled event is COMPLETED if the scheduled command or script started. The success of the schedule is independent of the success of the operation performed by the command or script.

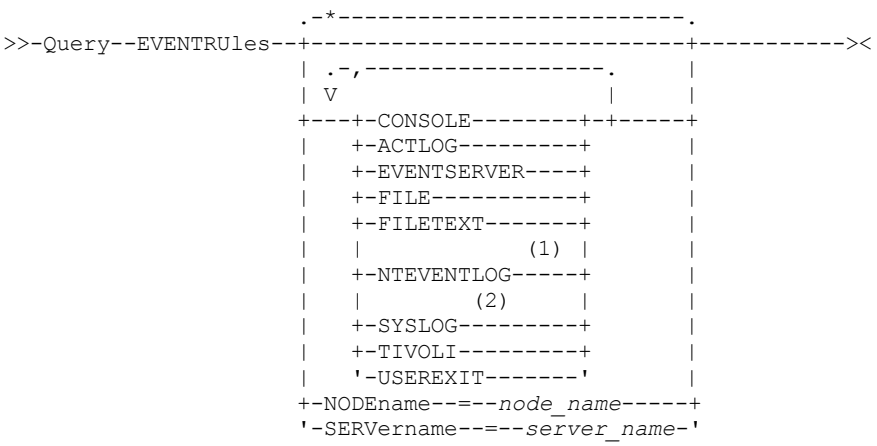
QUERY EVENTRULES (Query rules for server or client events)

Use this command to display the history of events that are enabled or disabled by a specified receiver for the server or for a client node.

Privilege class

Any administrator can issue this command.

Syntax



Notes:

1. This parameter is only available for the Windows operating system.
2. This parameter is only available for the Linux operating system.

Parameters

receivers
: Specifies the name of one or more receivers for enabled events. This parameter is optional.

  You can use a wildcard character to specify all receivers.

  Valid values are:

  CONSOLE
  : Specifies the standard console as a receiver.

  ACTLOG

Specifies the IBM Spectrum Protect™ activity log as a receiver.

EVENTSERVER
: Specifies the event server as a receiver.

FILE
: Specifies a user file as a receiver. Each logged event is a record in the file and a person cannot read each logged event easily.

FILETEXT
: Specifies a user file as a receiver. Each logged event is a fixed-size, readable line.

Windows NTEVENTLOG
: Windows Specifies the Windows application log as a receiver.

Linux SYSLOG
: Linux Specifies the Linux system log as a receiver.

TIVOLI
: Specifies the Tivoli Management Environment (TME) as a receiver.

USEREXIT
: Specifies a user-written routine to which IBM Spectrum Protect writes information as a receiver.

NODEname
: Specifies a node name to be queried. You can use a wildcard character to specify a name. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the query is for event rules for the server running this command.

SERver
: Specifies a server name to be queried. You can use a wildcard character to specify a name. You can specify NODENAME or SERVERNAME. If neither parameter is specified, the query is for event rules for the server running this command.

Example: Display the history of client events for the server console

Display the history of client events enabled or disabled for the server console and activity log receivers.

```
query eventrules console,actlog nodename=*

Date/Time            Client Event Rules
-------------------- ----------------------------------------------
05/29/97 13:39:58    ENABLE EVENTS CONSOLE ANE4001 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4962 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4963 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4965 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4966 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4967 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4968 NODENAMES=JEE
05/30/97 14:24:20    ENABLE EVENTS CONSOLE ANE4015 NODENAMES=RON
05/30/97 14:24:50    ENABLE EVENTS CONSOLE ANE4026 NODENAMES=DONNA
05/30/97 14:25:59    ENABLE EVENTS CONSOLE ANE4015 NODENAMES=DONNA
```

Example: Display the history of client events for all receivers

Display the history of server events enabled or disabled for all receivers.

```
query eventrules

Date/Time            Server Event Rules
-------------------- ----------------------------------------------
05/22/97 14:35:13    ENABLE EVENTS CONSOLE ANR2578
05/30/97 14:29:31    ENABLE EVENTS CONSOLE ANR0272
05/30/97 14:31:46    ENABLE EVENTS USEREXIT ANR0130
05/30/97 14:31:54    ENABLE EVENTS USEREXIT ANR0131
05/30/97 14:50:28    ENABLE EVENTS USEREXIT ANR0266
```

Field descriptions

Date/Time
: Specifies the date and time when the event was enabled or disabled.

Client Event Rules
: Specifies client events that were enabled or disabled for the specified receivers.

Server Event Rules
: Specifies server events that were enabled or disabled for the specified receivers.

Related commands

Table 1. Commands related to QUERY ENABLED

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DISABLE EVENTS	Disables specific events for receivers.
ENABLE EVENTS	Enables specific events for receivers.
END EVENTLOGGING	Ends event logging to a specified receiver.
QUERY ENABLED	Displays enabled or disabled events for a specific receiver.

QUERY EVENTSERVER (Query the event server)

Use this command to display the name of the event server.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query EVENTSERVer-----------------------------------------><
```

Example: Display the event server name

Display the name of the event server.

```
query eventserver
```

```
ANR1669I Server EVENT is defined as the event server.
```

Related commands

Table 1. Commands related to QUERY EVENTSERVER

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DEFINE EVENTSERVER	Defines a server as an event server.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE EVENTSERVER	Deletes reference to the event server.
DELETE SERVER	Deletes the definition of a server.
END EVENTLOGGING	Ends event logging to a specified receiver.

QUERY EXPORT (Query for active or suspended export operations)

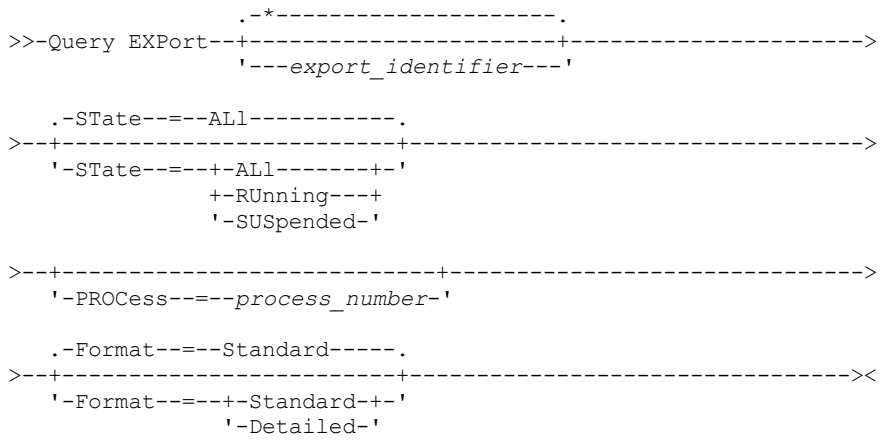
Use this command to list all restartable export operations. A restartable export is a server-to-server export operation whose FILEDATA value is not NONE. Only active server-to-server export operations that can be suspended are displayed.

Any EXPORT NODE or EXPORT SERVER operation with FILEDATA=NONE are not displayed. Additionally, the QUERY EXPORT command does not show export operations where the target device is either sequential media or virtual volumes.

Privilege class

An administrator can issue this command.

Syntax



Parameters

export_identifier
: This optional parameter is the unique string identifier for the server-to-server export operation. Wildcard characters can be used to specify this name, and all matching export operations are queried. If you do not specify a value for this parameter and you also do not specify a PROCESS identifier, then all export operations are queried.

STate
: This optional parameter queries the state of the valid server-to-server export operations. The default value is ALL. The possible values are:

  ALl
  : Lists all running and suspended server-to-server export operations.

  RUnning
  : Lists all active server-to-server export operations that are identifying eligible files or exporting files to the target server.

  SUSpended
  : Lists all suspended server-to-server export operations. These suspended operations stopped running because of a failure or by the SUSPEND EXPORT command being issued.

PROCess
: This optional parameter specifies the number of a running server-to-server export operation that you want to query. If PROCESS is specified, IBM Spectrum Protect™ only displays the running server-to-server export operation associated with the process number. If PROCESS is not specified, IBM Spectrum Protect displays information on all server-to-server export operations. You cannot specify this parameter if you specify an export identifier or if you specify the STATE parameter with a value of SUSPENDED.

Format
: This optional parameter specifies how the information is displayed. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the specified export operations.

  Detailed
  : When specified, displays all available information for the export operations.

Example: Display running and suspended export operations

List information for all currently running and suspended export operations. Issue the following command:

```
query export state=all
```

```
Export          Start Time    State      Process   Command
Identifier                                ID
-------------   -----------   ---------  --------  ------------------
MYEXPORTNODE    01/24/2007    Suspended     --     Export NODE
                10:30:03                           me,you,them
                                                   filespace=c$
```

```
                                                    nametype=unicode
                                                    filedata=all
                                                    durunits=indefinite
                                                    toserver=athens
                                                    exportid=MYEXPORTNODE

EXPORT_HOME_    01/25/2007   Running       11       Export NODE n2,n3,n4
DIRS            09:30:03                            filespace=/home
                                                    nametype=server
                                                    filedata=all
                                                    durunits=indefinite
                                                    toserver=athens
                                                    exportid=EXPORT_HOME_DIRS

EXPORT_NODE_    01/25/2007   Running Not   --       Export NODE n5,n6,n7
0001            14:30:33     Suspendible           filespace=d$
                                                    nametype=unicode
                                                    filedata=archive
                                                    durunits=indefinite
                                                    toserver=athens
```

See Field descriptions for field descriptions.

Example: Display information about a running export operation

List information for the currently running export operation with process number "7." Issue the following command:

```
query export process=7

Export        Start Time  State   Process  Command
Identifier                                 ID
----------    ----------  ------  ------   --------
MYEXPORTNODE  01/24/2007  Running   7      Export NODE
              10:30:03                     me,you,them
                                           filespace=c$
                                           nametype=unicode
                                           filedata=all
                                           toserver=athens
                                           exportid=MYEXPORTNODE
```

See Field descriptions for field descriptions.

Example: Display detailed information about all suspended export operations

List information for all currently suspended export operations. Issue the following command:

```
query export state=suspended format=detailed

             Export Identifier: MyExportNode
                    Start Time: 01/24/2007 10:30:03
                         State: Suspended
                    Process Id: --
                       Command: Export NODE m* filespace=c$
                                 nametype=unicode
                                 filedata=all durunits=indefinite
                                 toserver=athens
                         Phase: File list complete. Exporting
                                 eligible files
           Total Running Time: 3 Days 0 Hours 24 Minutes
  Current Process Running Time:
Export Operation Restart Count: 0
 Date and Time of Last Restart: --
 Date and Time of Last Suspend: 01/25/2007 08:30:11
       Policy Domains Exported: 0
          Policy Sets Exported: 0
            Schedules Exported: 0
         Mgmt Classes Exported: 0
          Copy Groups Exported: 0
       Administrators Exported: 1
          Option Sets Exported: 0
     Node Definitions Exported: 3
Filespace Definitions Exported: 7
        Archive Files Exported: 50,000
```

```
        Backup Files Exported: 150,000
  Space Managed Files Exported: 0
         Archive Files Skipped: 0
          Backup Files Skipped: 25
   Space Managed Files Skipped: 0
  Total bytes Transferred (MB): 7,000
 Total Files to be Transferred: 900,000
               Files Remaining: 700,000
```

See Field descriptions for field descriptions.

Example: Display information for server-to-server export operations

List detailed information for all currently running server-to-server export operations. Issue the following command:

```
query export state=running format=detailed
```

```
             Export Identifier: export_HOME_Dirs
                    Start Time: 01/25/2007 09:30:03
                         State: Running
                    Process Id: 11
                       Command: Export NODE n2,n3,n4
                                filespace=/home nametype=
                                server filedata=all
                                toserver=athens
                         Phase: Identifying and exporting
                                eligible files
           Total Running Time: 0 Days 22 Hours 0 Minutes
  Current Process Running Time: 01:30:00
Export Operation Restart Count: 4
 Date and Time of last Restart: 02/01/2007 11:00:03
 Date and Time of last Suspend: 01/31/2007 05:01:00
       Policy Domains Exported: 0
          Policy Sets Exported: 0
            Schedules Exported: 0
         Mgmt Classes Exported: 0
           Copy Groups Exported: 0
       Administrators Exported: 1
          Option Sets Exported: 0
     Node Definitions Exported: 3
Filespace Definitions Exported: 7
        Archive Files Exported: 0
         Backup Files Exported: 1000
  Space Managed Files Exported: 0
         Archive Files Skipped: 0
          Backup Files Skipped: 0
   Space Managed Files Skipped: 0
  Total bytes Transferred (MB): 50
 Total Files to be Transferred: 400,000
               Files Remaining: 399,000
```

See Field descriptions for field descriptions.

Field descriptions

Export identifier
: The unique identifier assigned to this server-to-server export operation.

Start time
: The time and date that this export operation was first initiated.

State
: The current state of this export operation. The value is one of the following:

  Running - Not Suspendible
  : The operation is active and is transmitting definitions to the target server. The process cannot be suspended, and if the process fails while in this state, you cannot restart it.

  Running
  : The operation is active and is either searching for eligible files or transmitting file data to the target server.

  Running - Suspend in Progress
  : The operation is in the process of being suspended as a result of a SUSPEND EXPORT command. The export operation is fully suspended when all of the data from the export operation is saved. An export operation in this state

does not respond to the following commands:

- CANCEL PROCESS
- CANCEL EXPORT
- RESTART EXPORT
- SUSPEND EXPORT

Suspended
: The operation stopped running due to a failure or was suspended with the SUSPEND EXPORT command.

Process ID
: The process ID for the export operation when the status is either "Initializing" or "Running".

Command
: The full command issued to start this server-to-server export.

Phase
: The current step that the operation is performing. The possible phases are shown in the order in which they are performed:

  Creating definitions on target server
  : The operation is exporting definitions. The process cannot be suspended. Should the process fail in this phase, it cannot be restarted.

  Identifying and exporting eligible files
  : The operation is building a list of eligible files for export. Some files may also be transmitted to the target during this phase. A process in this phase can be suspended. Should the process fail in this phase, it can be restarted.

  File list complete. Exporting eligible files
  : The operation has completed building the list of eligible files for export and it is now transmitting the files to the target. A process in this phase can be suspended. Should the process fail in this phase, it can be restarted.

Total running time
: The overall running time for this server-to-server export operation. For example, if this operation started and was then suspended and restarted two times, this value is the total running time of all three active processes of the export operation.

Current® process running time
: The running time of the active process of a server-to-server export operation. No value is displayed for a suspended operation because no active process exists.

Export operation restart count
: The number of times the server-to-server export operation was restarted.

Date and time of last restart
: The last date and time at which this server-to-server export operation was restarted.

Date and time of last suspend
: The last date and time at which this server-to-server export operation was suspended.

Policy domains exported
: The number of policy domain definitions successfully exported to the target server.

Policy sets exported
: The number of policy set definitions successfully exported to the target server.

Schedules exported
: The number of schedule definitions successfully exported to the target server.

Mgmt classes exported
: The number of management class definitions successfully exported to the target server.

Copy groups exported
: The number of copy group definitions successfully exported to the target server.

Administrators exported
: The number of administrator definitions successfully exported to the target server.

Option sets exported
: The number of option set definitions successfully exported to the target server.

Node definitions exported
: The number of node definitions successfully exported to the target server.

File space definitions exported
: The number of file space definitions successfully exported to the target server.

Archive files exported
: The number of archive files successfully exported to the target server.

Backup files exported
: The number of backup files successfully exported to the target server.

Space managed files exported
: The number of space managed files successfully exported to the target server.

Archive files skipped
: The number of archive files that were eligible for export but were skipped.

Backup files skipped
: The number of backup files that were eligible for export but were skipped.

Space managed files skipped
: The number of space managed files that were eligible for export but were skipped.

Total bytes transferred (MB)
: The total number of bytes transmitted so far to the target server for this export operation.

Total files to be transferred
: The total number of files transmitted so far to the target server for this export operation.

Files remaining
: The total number of files remaining to be transmitted to the target server for this export operation.

Related commands

Table 1. Commands related to QUERY EXPORT

Command	Description
CANCEL PROCESS	Cancels a background server process.
CANCEL EXPORT	Deletes a suspended export operation.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
IMPORT NODE	Restores client node information from external media.
IMPORT SERVER	Restores all or part of the server from external media.
QUERY PROCESS	Displays information about background processes.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

AIX | Linux | Windows

QUERY EXTENTUPDATES (Query updated data extents)

Use this command to display information about updates to data extents in directory-container storage pools and to determine what data extents are deleted and what is eligible for deletion.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query EXTENTUPDates--pool_name-----------------------------><
```

Parameters

pool_name (Required)
: Specifies the storage pool to query. You cannot use wildcards to specify this name.

Example: Display information about updates to data extents

Display information about updates to data extents by issuing the following command:

```
query extentupdates
```

```
     Number of Extents Pending Update: 0
        Number of Extents Not Referenced: 0
 Number of Extents Eligible for Deletion: 0
               Extent Reuse Delay (Days): 1
```

See Field descriptions for field descriptions.

Field descriptions

Number of Extents Pending Update
: Specifies the number of data extent references that are pending an update in the directory-container storage pool. Data that is stored in the directory-container storage pool increases the number of references and data deletion decreases the number of references.

Number of Extents Not Referenced
: Specifies the number of data extents that are not referenced in the directory-container storage pool. You can delete the data extents if they are not referenced again within the reuse delay period that is specified on the DEFINE STGPOOL command.

Number of Extents Eligible for Deletion
: Specifies the number of data extents that can be deleted from the storage pool. The data extents exceed the reuse delay period that is specified on the DEFINE STGPOOL command.

Extent Reuse Delay (Days)
: Specifies the reuse delay time, in days, for data extents.

Related commands

Table 1. Commands related to QUERY EXTENTUPDATES

Command	Description
DEFINE STGPOOL (directory-container)	Define a directory-container storage pool.
DELETE STGPOOLDIRECTORY	Deletes a storage pool directory from a directory-container or cloud-container storage pool.

QUERY FILESPACE (Query one or more file spaces)

Use this command to display information about file spaces that belong to a client node. The output from this command includes the results of the last incremental backup or replication.

Tip: If a node has more than one file space, you can issue a DELETE FILESPACE command for one of the file spaces. However, if you issue a QUERY FILESPACE command for the node during the deletion process, the output shows no file spaces. To obtain accurate information about remaining file spaces, issue the QUERY FILESPACE command after the deletion process ends.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*--*---------------------------.
>>-Query FIlespace--+-----------------------------------+----------><
                    |            .-*---------------. |
                    '-node_name--+-----------------+-'
                                 '-file_space_name-'

   .-Format--=--Standard-----.  .-NAMEType--=--SERVER------.
>--+-------------------------+--+-------------------------+----><
   '-Format--=--+-Standard-+-'  '-NAMEType--=--+-SERVER--+-'
                '-Detailed-'                   +-UNIcode-+
                                               '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+----------------------------><
   '-CODEType--=--+-UNIcode----+-'
                  +-NONUNIcode-+
```

```
'-BOTH-------'
```

Parameters

node_name
: Specifies the client node to which the file space belongs. You can use wildcard characters to specify this name. This parameter is optional. The default is all client node names.

  You must specify a value for this parameter if you specify a file name.

file_space_name
: Specifies the name of the file space to be queried. You can use wildcard characters to specify this name. This parameter is optional. If a value is not specified, all file spaces are queried.

  If a server includes clients that use Unicode-enabled files spaces, the server might have to convert the name that you enter. For example, the server might have to convert the file space name that you enter from the server code page to Unicode. For more information, see the NAMETYPE parameter. If you do not specify a file space name, or if you specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

  File space names are case-sensitive. You can use the QUERY FILESPACE command to determine the correct capitalization for the file space to be queried.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. You can specify one of the following values:

  Standard
  : Specifies that partial information is displayed for the specified file space.

  Detailed
  : Specifies that complete information is displayed for the specified file space.

NAMEType
: Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect™ clients that have Windows, Macintosh OS X, and NetWare operating systems.

  Use this parameter only when you enter a partly qualified or fully qualified file space name. The default value is SERVER. You can specify one of the following values:

  SERVER
  : The server uses the server code page to interpret the file space names.

  UNIcode
  : The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has problems accessing system conversion routines.

  FSID
  : The server interprets the file space names as their file space IDs (FSIDs).

CODEType
: Specify what type of file spaces are to be included in the operation. The default is BOTH, meaning that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name. You can specify one of the following values:

  UNIcode
  : Include only file spaces that are in Unicode.

  NONUNIcode
  : Include only file spaces that are not in Unicode.

  BOTH
  : Include file spaces regardless of code page type.

Example: List all file spaces

Query all file spaces that are associated with all client nodes.

```
query filespace

Node   Filespace   FSID  Platform  Filespace    Is     Capacity Pct
Name   Name                        Type      Filespace          Util
                                             Unicode?
------ ----------- ----  --------  --------  --------  -------- ----
JOE    \\joe\c$       1  WinNT     NTFS        Yes     2,502.3  75.2
JOE    \\joe\d$       2  WinNT     NTFS        Yes     6,173.4  59.6
```

See Field descriptions for field descriptions.

Example: Display detailed file space information for a virtual file space

Display detailed information for the file space /HomeDir, which is a virtual file space mapping and belongs to the NAS node NAS1.

```
query filespace nas1 /HomeDir

Node   Filespace   FSID  Platform  Filespace     Is     Capacity Pct
Name   Name                        Type      Filespace          Util
                                              Unicode?
----   ----------- ----  --------  --------  ---------  -------- ----
NAS1   /HomeDir     1    NetApp    WAFL (VFS)     No     2,502.3  75.2
```

See Field descriptions for field descriptions.
Important: You might not see the expected results after you request a detailed format because several fields must be completed by the API application. These fields include:

- File space type
- Platform
- Capacity
- Pct Util
- Last backup start Date/Time
- Last backup completion Date/Time

For more information about specific fields that are updated by the API, see the *IBM Spectrum Protect: Using the Application Programming Interface*.

Example: Display detailed file space information for a specific file space and node

Display detailed information about the \\joe\c$ file space that belongs to the client node JOE.

```
query filespace joe \\joe\c$ nametype=unicode format=detailed

                                 Node Name: JOE
                            Filespace Name: \\joe\c$
                  Hexadecimal Filespace Name: 5c5c6a6f655c6324
                                        FSID: 1
                      Collocation Group Name: FSGRP1
                                    Platform: WinNT
                            Filespace Type: NTFS
                     Is Filespace Unicode?: Yes
                                    Capacity: 2,502.3
                                    Pct Util: 75.2
                Last Backup Start Date/Time:
             Days Since Last Backup Started:
           Last Backup Completion Date/Time:
           Days Since Last Backup Completed:
           Last Replication Start Date/Time: 12/02/2012, 12:42:00
Days Since Last Node Replication Started: 30
   Last Replication Completion Date/Time: 12/02/2012, 12:42:00
   Days Since Last Replication Completed: 30
 Last Backup Date/Time From Client (UTC): 06/02/2013, 09:10:00
Last Archive Date/Time From Client (UTC): 06/02/2013, 09:10:00
            Backup Replication Rule Name: ACTIVE_DATA
           Backup Replication Rule State: ENABLED
           Archive Replication Rule Name: DEFAULT
          Archive Replication Rule State: ENABLED
  Space Management Replication Rule Name: NONE
 Space Management Replication Rule State: DISABLED
```

```
          At-risk type: Custom interval
       At-risk interval: 2,222
         Decommissioned: No
    Decommissioned Date:
           MAC Address:
```

See Field descriptions for field descriptions.

Field descriptions

Important: You might not see the expected results after requesting a detailed format because several fields must be completed by the API application. These fields include:

- Filespace Type
- Platform
- Capacity
- Pct Util
- Last Backup Start Date/Time
- Last Backup Completion Date/Time

For more information about specific fields that are updated by the API, see the *IBM Spectrum Protect: Using the Application Programming Interface*.

Node Name
: Specifies the name of the client node.

Filespace Name

: The name of the file space that belongs to the node.

  File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

  If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

Hexadecimal Filespace Name
: Specifies the hexadecimal name of the file space for the client node in UTF-8 format.

FSID
: Specifies the file space ID of the file space.

Collocation Group Name
: The name of the collocation group, if any, to which the file space belongs.

Platform
: Specifies the platform for the client node.

Filespace Type
: Specifies the type of file space.

  A file space type that is appended with "(VFS)" denotes that this file space name is a virtual file space mapping for a directory path on a NAS device.

Is Filespace Unicode?
: Indicates whether the file space is Unicode.

Capacity
: Specifies the amount of space, in megabytes, assigned to this file space on the client node.

  For a file space that is a virtual file space mapping for a directory path, this field represents the capacity of the file space on which the directory path is located.

Pct Util
: Specifies the percentage of the file space that is occupied.

  For a file space that is a virtual file space mapping for a directory path, the percentage used is calculated as the percentage of the capacity of the file space that was occupied by the directory at the time of the last full backup.

Last Backup Start Date/Time
Specifies the start date and time of the last incremental backup of the file space.
Days Since Last Backup Started
Specifies the number of days since the start of the last incremental backup of the file space.
Last Backup Completion Date/Time
Specifies the completion date and time of the last incremental backup of the file space.
Days Since Last Backup Completed
Specifies the number of days since the completion of the last incremental backup of the file space.
Last Replication Start Date/Time
Specifies the date and time that the last replication of file space data started.
Days Since Last Replication Started
Specifies the number of days since the last replication of file space data started.
Last Replication Completion Date/Time
Specifies the date and time that the last replication of file space data ended.
Days Since Last Replication Completed
Specifies the number of days since the last replication of file space data ended.
Last Backup Date/Time From Client (UTC)
The date and time, in Universal Time Coordinates (UTC), of the last backup operation for this file space.
Last Archive Date/Time From Client (UTC)
The date and time, in Universal Time Coordinates (UTC), of the last archive operation for this file space.
Backup Replication Rule Name
Specifies the replication rule that applies to backup data in the file space. The following values are possible:

ALL_DATA
Replicates active and inactive backup data. The data is replicated with a normal priority.
ACTIVE_DATA
Replicates only active backup data. The data is replicated with a normal priority.
Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

- When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
- When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
- When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.
ALL_DATA_HIGH_PRIORITY
Replicates active and inactive backup data. The data is replicated with a high priority.
ACTIVE_DATA_HIGH_PRIORITY

This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

DEFAULT
Replicates backup data according to the client node rule for backup data. If the client node rule for backup data is DEFAULT, backup data is replicated according to the server rule for backup data.
NONE
Backup data in the file space is not replicated.

Backup Replication Rule State
Specifies whether replication of backup data in the file space is enabled or disabled. If the state is ENABLED, backup files are eligible for replication. If the state is DISABLED, backup files are not eligible for replication.
Archive Replication Rule Name
Specifies the replication rule that applies to archive data in the file space. The following values are possible:

ALL_DATA
Replicates archive data. The data is replicated with a normal priority.
ALL_DATA_HIGH_PRIORITY
Replicates archive data. The data is replicated with a high priority.
DEFAULT
Replicates archive data according to the client rule for archive data. If the client rule for archive data is DEFAULT, archive data is replicated according to the server rule for archive data.
NONE
Archive data in the file space is not replicated.

Archive Replication Rule State
: Specifies whether replication of archive data in the file space is enabled or disabled. If the state is ENABLED, archive files are eligible for replication. If the state is DISABLED, archive files are not eligible for replication.

Space Management Replication Rule Name
: Specifies the replication rule that applies to space-managed data in the file space. The following values are possible:

  ALL_DATA
  : Replicates space-managed data. The data is replicated with a normal priority.

  ALL_DATA_HIGH_PRIORITY
  : Replicates space-managed data. The data is replicated with a high priority.

  DEFAULT
  : Replicates space-managed data according to the client rule for space-managed data. If the client rule for space-managed data is DEFAULT, space-managed data is replicated according to the server rule for space-managed data.

  NONE
  : Space-managed data in the file space is not replicated.

Space Management Replication Rule State
: Specifies whether replication of space-managed data in the file space is enabled or disabled. If the state is ENABLED, space-managed files are eligible for replication. If the state is DISABLED, space-managed files are not eligible for replication.

At-risk type
: Specifies the at-risk evaluation type. Values can be Default, Bypassed, or Custom. Default indicates that the node is evaluated with the same interval that was specified for the nodes classification by the SET STATUSATRISKINTERVAL command. Bypassed indicates that the node is not evaluated for at-risk status by the status monitor. Custom indicates that the node is evaluated with the interval that was specified by the SET VMATRISKINTERVAL command, rather than the interval that was specified by the SET STATUSATRISKINTERVAL command.

At-risk interval
: Specifies the amount of time, in hours, between client backup activity before the status monitor considers the client at-risk. This field applies only when the at-risk type is Custom.

Decommissioned
: Specifies whether the virtual machine that the file space represents is decommissioned.

Decommissioned Date
: Specifies the date that the virtual machine that the file space represents was decommissioned.

MAC Address
: Specifies the media access control (MAC) address of the file spaces backed up for VMWare virtual machines. In the case where the virtual machine has multiple MAC addresses this is the lowest valued address.

Related commands

Table 1. Commands related to QUERY FILESPACE

Command	Description
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
RENAME FILESPACE	Renames a client filespace on the server.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE NODE	Changes the attributes that are associated with a client node.

QUERY FSCOUNTS (Query number of objects)

Use this command to display information about the number of objects (files and directories) in file spaces that belong to a client node.

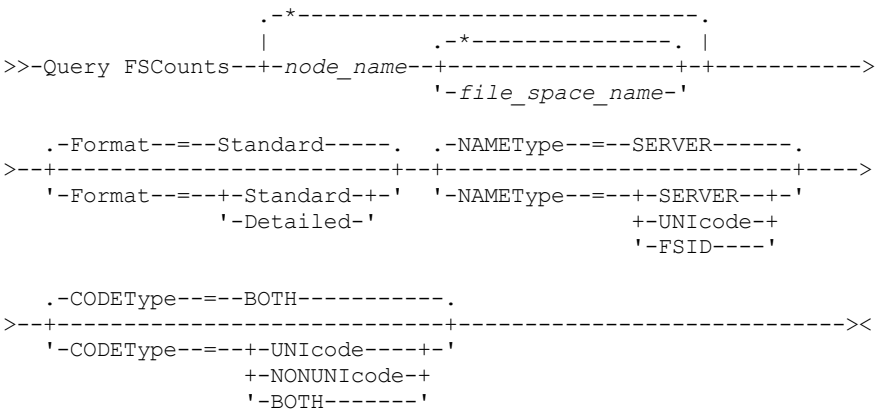
Tip: To obtain accurate information, issue the QUERY FSCOUNTS command after the backup operations ends. Also, if you are currently expiring objects from the file space, the numbers might not reflect the latest changes.

The database is queried and the counts are completed in real time.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

node_name
: Specifies the client node to which the file space belongs. You can use wildcard characters to specify this name, or use a group name. A group name specifies the name of the group to which the client node belongs. This parameter is required. Comma-delimited lists are not allowed. An asterisk specifies all client nodes.

NAMEType
: Specifies how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect™ clients that have Windows, Macintosh OS X, and NetWare operating systems.

  Use this parameter only when you enter a partly qualified or fully qualified file space name. The default value is SERVER. You can specify one of the following values:

  SERVER
  : The server uses the server code page to interpret the file space names.

  UNIcode
  : The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has problems accessing system conversion routines.

  FSID
  : The server interprets the file space names as their file space IDs (FSIDs).

CODEType
: Specifies what type of file spaces are to be included in the operation. The default is BOTH, meaning that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name. You can specify one of the following values:

  UNIcode
  : Include only file spaces that are in Unicode.

  NONUNIcode
  : Include only file spaces that are not in Unicode.

  BOTH
  : Include file spaces regardless of code page type.

Field descriptions

Node Name
: Specifies the name of the client node.

FSID
: Specifies the file space ID of the file space.

Filespace Type
: Specifies the type of file space.

  A file space type that is appended with "(VFS)" denotes that this file space name is a virtual file space mapping for a directory path on a network-attached storage (NAS) device.

Is Filespace Unicode?
: Indicates whether the file space is Unicode.

Related commands

Table 1. Commands related to QUERY FSCOUNTS

Command	Description
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY OCCUPANCY	Displays file space information by storage pool.

QUERY LIBRARY (Query a library)

Use this command to display information about libraries.

Privilege class

Any administrator can issue this command.

Syntax

```
                  .-*------------.
>>-Query LIBRary--+--------------+------------------------------>
                  '-library_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

library_name
: Specifies the name of the library to be queried. You can use wildcards to specify names. This parameter is optional.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the library.

  Detailed
  : Specifies that complete information is displayed for the library.

Example: Display summary information about a specific library

Display information about the library named AUTO. Issue the command:

```
query library auto
```

```
         Library Name: AUTO
         Library Type: SCSI
               ACS Id:
     Private Category:
     Scratch Category:
WORM Scratch Category:
     External Manager:
               Shared: No
             LanFree:
   ObeyMountRetention:
```

See Field descriptions for field descriptions.

Example: Display detailed library information about a specific library

Display information in full detail about the library named EZLIFE. Issue the command: AIX Linux

```
query library ezlife format=detailed
```

AIX Linux

```
                  Library Name: EZLIFE
                  Library Type: SCSI
                        ACS Id:
               Private Category:
               Scratch Category:
          WORM Scratch Category:
               External Manager:
                        Shared: Yes
                      LanFree:
           ObeyMountRetention:
       Primary Library Manager: EZSERVER
                           WWN:
                 Serial Number:
                     AutoLabel: OVERWRITE
                Relabel Scratch: Yes
Last Update by (administrator): DOCTOR_MIKE
         Last Update Date/Time: 2002-12-05 15:24:53
```

Windows

```
                  Library Name: EZLIFE
                  Library Type: SCSI
                        ACS Id:
               Private Category:
               Scratch Category:
          WORM Scratch Category:
               External Manager:
                        Shared: YES
                      LanFree:
           ObeyMountRetention:
       Primary Library Manager: EZSERVER
                           WWN:
                 Serial Number:
                     AutoLabel: OVERWRITE
                  Reset Drives: No
                Relabel Scratch: Yes
Last Update by (administrator): DOCTOR_MIKE
         Last Update Date/Time: 2000-12-05 15:24:53
```

See Field descriptions for field descriptions.

Field descriptions

Library Name
: The name of the library.

Library Type
: The type of library.

ACS Id
: Specifies that the library is a StorageTek library that is controlled by StorageTek Automated Cartridge System Library Software (ACSLS).

Private Category

The category number for private volumes that must be mounted by name.

The information that is displayed in this field applies only to an IBM® 3494 or 3495 Tape Library Dataserver.

Scratch Category
: The category number to use for scratch volumes in the library.

The information that is displayed in this field applies only to an IBM 3494 or 3495 Tape Library Dataserver.

WORM Scratch Category
: The category number that is used for WORM scratch volumes in the library.

The information that is displayed in this field applies only to an IBM 3494 or 3495 Tape Library Dataserver.

External Manager
: The location of the external library manager where the server can send media access requests.

Shared
: Whether this library is shared with other IBM Spectrum Protect™ servers in a storage area network (SAN).

LanFree
: Whether an external library is used for LAN-free operations.

ObeyMountRetention
: Whether the server uses the value that is set for mount retention in the device class that is associated with this external library.

Primary Library Manager
: The name of the server that is responsible for controlling access to library resources.

WWN
: The Fibre Channel worldwide name for the library.

Serial Number
: Specifies the serial number for the library that is being queried.

AutoLabel
: Specifies whether the server attempts to automatically label tape volumes.

AIX Windows Reset Drives
: AIX Windows Specifies whether the server completes a target reset when the server is restarted or when a library client or storage agent re-connection is established.

Relabel Scratch
: Specifies whether the server relabels volumes that were deleted and returned to scratch.

Last Update by (administrator)
: Who completed the last update to the library.

Last Update Date/Time
: The date and time when the last update occurred.

Related commands

Table 1. Commands related to QUERY LIBRARY

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE LIBRARY	Deletes a library.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE LIBRARY	Changes the attributes of a library.

QUERY LIBVOLUME (Query a library volume)

Use this command to display information about one or more volumes that are checked into an automated library for use by the IBM Spectrum Protect™ server.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*------------.  .-*-----------.
>>-Query LIBVolume--+--------------+--+-------------+----------->
                    '-library_name-'  '-volume_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

library_name
: Specifies the name of the library. You can use wildcard characters to specify this name. This parameter is optional. The default is all libraries.

volume_name
: Specifies the volume name. You can use wildcard characters to specify this name. This parameter is optional. The default is all volumes.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: List checked in volumes for a specific library

Display information about all of the volumes that are checked into the library named TAPE. See Field descriptions for field descriptions.

```
query libvolume tape
```

```
Library Name  Volume Name  Status   Owner   Last Use   Home     Device
                                                      Element  Type
------------  -----------  -------- ------- --------   ------  ------
TAPE          000114       Scratch                     1,000    LTO
TAPE          NY1602       Scratch                     1,001    DLT
```

Example: Display detailed information for a specific library

Display detailed information about a volume named JJY008. See Field descriptions for field descriptions.

```
query libvolume jjy008 format=detailed
```

```
                         Library Name: HPW3494
                          Volume Name: JJY008
                               Status: Private
                                Owner: SUNSET
                            Last Use: Data
                         Home Element:
                          Device Type:
                        Cleanings Left:
                            Media Type:
```

Field descriptions

Library Name
: The name of the library where the storage volume is located.

Volume Name
: The name of the storage volume.

Status

The status of the storage volume according to the library inventory. If the status is Private, the volume is being used by IBM Spectrum Protect. If the status is Scratch, the volume is available for use.

Owner
: The owner server of the volume, if the volume is private.

Last Use
: The type of data on the volume. This field applies only to volumes in Private status. For storage pool volumes, this field shows **Data**. For database backup volumes (full, incremental, or snapshot), this field shows **DbBackup**.

Home Element
: The element address of the library slot containing the volume.

Device Type
: The type of device that the volume is used on. This field will display a value only for volumes checked into a library that has mixed media capabilities.

Cleanings Left
: For cleaner cartridges, the number of cleanings left.

Media Type
: The type of media the volume represents (for example, 8mm tape).

Related commands

Table 1. Commands related to QUERY LIBVOLUME

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
QUERY LIBRARY	Displays information about one or more libraries.
UPDATE LIBVOLUME	Changes the status of a storage volume.

QUERY LICENSE (Display license information)

Use this command to display license audit, license terms, and compliance information.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query LICense-----------------------------------------------><
```

Parameters

None.

To display the license information, issue the following command:

```
query license
```

The following example output is displayed:

```
                          ANR2017I Administrator
                      SERVER_CONSOLE issued command: QUERY LICENSE
                                Last License Audit: 10/17/2016
                                                    14:28:08
       Number of Data Protection for Oracle in use: 0
                      Number of Data Protection for
                             Oracle in try buy mode: 0
 Number of Data Protection for Microsoft SQL in use: 0
                      Number of Data Protection for
                      Microsoft SQL in try buy mode: 0
                      Number of Data Protection for
                          Microsoft Exchange in use: 0
                      Number of Data Protection for
                        MS Exchange in try buy mode: 0
             Number of TDP for Lotus Notes in use: 12
     Number of TDP for Lotus Notes in try buy mode: 0
  Number of Data Protection for Lotus Domino in use: 0
                      Number of Data Protection for
                       Lotus Domino in try buy mode: 0
                  Number of TDP for Informix in use: 1
         Number of TDP for Informix in try buy mode: 0
                    Number of TDP for SAP R/3 in use: 0
          Number of TDP for SAP R/3 in try buy mode: 0
                        Number of TDP for ESS in use: 0
              Number of TDP for ESS in try buy mode: 0
                   Number of TDP for ESS R/3 in use: 0
           Number of TDP for ESS R/3 in try buy mode: 0
              Number of TDP for EMC Symmetrix in use: 0
    Number of TDP for EMC Symmetrix in try buy mode: 0
         Number of TDP for EMC Symmetrix R/3 in use: 6
Number of TDP for EMC Symmetrix R/3 in try buy mode: 0
                      Number of TDP for WAS in use: 0
             Number of TDP for WAS in try buy mode: 0
  Is IBM Spectrum Protect for Data Retention in use?: No
Is IBM Spectrum Protect for Data Retention licensed?: Yes
       Is IBM Spectrum Protect Basic Edition in use: Yes
     Is IBM Spectrum Protect Basic Edition licensed: Yes
    Is IBM Spectrum Protect Extended Edition in use: No
  Is IBM Spectrum Protect Extended Edition licensed: Yes
                         Server License Compliance: Valid
```

Field descriptions

Last License Audit
: Specifies the date and time when the last license audit occurred.

Number of Data Protection for Oracle in use
: Specifies the number of Data Protection for Oracle that are in use. A product is in use if you purchased the product and registered the license.

Number of Data Protection for Oracle in try buy mode
: Specifies the number of Data Protection for Oracle that are in try buy mode.

Number of Data Protection for Microsoft SQL in use
: Specifies the number of Data Protection for Microsoft SQL that are in use. A product is in use if you purchased the product and registered the license.

Number of Data Protection for Microsoft SQL in try buy mode
: Specifies the number of Data Protection for Microsoft SQL that are in try buy mode.

Number of Data Protection for Microsoft Exchange in use
: Specifies the number of Data Protection for Microsoft Exchange that are in use. A product is in use if you purchased the product and registered the license.

Number of Data Protection for Microsoft Exchange in try buy mode
: Specifies the number of Data Protection for Microsoft Exchange that are in try buy mode.

Number of TDP for Lotus Notes® in use
: Specifies the number of TDP for Lotus Notes that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for Lotus Notes in try buy mode
: Specifies the number of TDP for Lotus Notes that are in try buy mode.

Number of Data Protection for Lotus® Domino® in use
: Specifies the number of Data Protection for Lotus Domino that are in use. A product is in use if you purchased the product and registered the license.

Number of Data Protection for Lotus Domino in try buy mode
: Specifies the number of Data Protection for Lotus Domino that are in try buy mode.

Number of TDP for Informix® in use
: Specifies the number of TDP for Informix that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for Informix in try buy mode
: Specifies the number of TDP for Informix that are in try buy mode.

Number of TDP for SAP R/3 in use
: Specifies the number of TDP for SAP R/3 that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for SAP R/3 in try buy mode
: Specifies the number of TDP for SAP R/3 that are in try buy mode.

Number of TDP for ESS in use
: Specifies the number of TDP for ESS that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for ESS in try buy mode
: Specifies the number of TDP for ESS that are in try buy mode.

Number of TDP for ESS R/3 in use
: Specifies the number of TDP for ESS R/3 that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for ESS R/3 in try buy mode
: Specifies the number of TDP for ESS R/3 that are in try buy mode.

Number of TDP for EMC Symmetrix in use
: Specifies the number of TDP for EMC Symmetrix that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for EMC Symmetrix in try buy mode
: Specifies the number of TDP for EMC Symmetrix that are in try buy mode.

Number of TDP for EMC Symmetrix R/3 in use
: Specifies the number of TDP for EMC Symmetrix R/3 that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for EMC Symmetrix R/3 in try buy mode
: Specifies the number of TDP for EMC Symmetrix R/3 that are in try buy mode.

Number of TDP for WAS in use
: Specifies the number of TDP for WAS that are in use. A product is in use if you purchased the product and registered the license.

Number of TDP for WAS in try buy mode
: Specifies the number of TDP for WAS that are in try buy mode.

Is IBM Spectrum Protect™ for Data Retention in use ?
: Specifies whether the IBM Spectrum Protect for Data Retention is in use. A product is in use if you purchased the product and registered the license.

Is IBM Spectrum Protect for Data Retention licensed ?
: Specifies whether the IBM Spectrum Protect for Data Retention is licensed.

Is IBM Spectrum Protect Basic Edition in use
: Specifies whether the IBM Spectrum Protect Basic Edition is in use. A product is in use if you purchased the product and registered the license.

Is IBM Spectrum Protect Basic Edition licensed
: Specifies whether the IBM Spectrum Protect Basic Edition is licensed.

Is IBM Spectrum Protect Extended Edition in use
: Specifies whether the IBM Spectrum Protect Extended Edition is in use. A product is in use if you purchased the product and registered the license.

Is IBM Spectrum Protect Extended Edition licensed
: Specifies whether the IBM Spectrum Protect Extended Edition is licensed.

Server License Compliance
: Specifies whether the server license is valid.

Related commands

Table 1. Commands related to QUERY LICENSE

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.

Command	Description
QUERY AUDITOCCUPANCY	Displays the server storage utilization for a client node.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY PVUESTIMATE	Displays processor value unit estimates. Remember: The QUERY PVUESTIMATE command reports licenses by providing PVU information on a per-node basis for server devices.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER LICENSE	Registers a license with the IBM Spectrum Protect server.
REGISTER NODE	Defines a client node to the server and sets options for that user.
SET CPUINFOREFRESH	Specifies the number of days between client scans for workstation information used for PVU estimates.
SET LICENSEAUDITPERIOD	Specifies the number of days between automatic license audits.
UPDATE NODE	Changes the attributes that are associated with a client node.

QUERY LOG (Display information about the recovery log)

Use this command to display information about the recovery log.

Privilege class

Any administrator can issue this command.

Syntax

```
              .-Format--=--Standard-----.
>>-Query LOG--+-------------------------+----------------------><
              '-Format--=--+-Standard-+-'
                           '-Detailed-'
```

Parameters

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. The following values are possible:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display summary information about the recovery log

Display summary information about the recovery log. See Field descriptions for field descriptions.

```
query log

Total Space (MB)    Used Space (MB)     Free Space (MB)
----------------    ---------------     ---------------
          38,912              543.3            38,368.7
```

AIX | Linux

Example: Display detailed information about the recovery log

Display detailed information about the recovery log. See Field descriptions for field descriptions.

```
query log format=detailed
```

```
                     Active Log Directory : /actlog
                          Total Space (MB): 524,032
                           Used Space (MB): 3,517
                           Free Space (MB): 520,515

              Total Size of File System (MB): 564,443
              Used Space on File System (MB): 527,049
              Free Space on File System (MB): 8,722

                      Archive Log Directory : /archlog
              Total Size of File System (MB): 603,751.82
              Used Space on File System (MB): 80,642.30
              Free Space on File System (MB): 523,109.52
                     Archive Log Compressed : Yes

                       Mirror Log Directory : /mirrorlog
              Total Size of File System (MB): 564,443
              Used Space on File System (MB): 527,049
              Free Space on File System (MB): 8,722

            Archive Failover Log Directory : /archfaillog
              Total Size of File System (MB): 301,372.06
              Used Space on File System (MB): 44,741.80
              Free Space on File System (MB): 256,630.26
```

Windows

Example: Display detailed information about the recovery log when the mirror log and the archive failover log are not defined

The output of this command on Windows systems is different. For example, the output contains blanks for the mirror log and the archive failover log.
Display information about the recovery log when the mirror log and the archive failover log are not defined.

```
query log format=detailed
```

Windows

```
                  Active Log Directory : d:\actlog
                       Total Space (MB): 524,032
                        Used Space (MB): 3,517
                        Free Space (MB): 520,515

          Total Size of File System (MB): 564,443
          Used Space on File System (MB): 527,049
          Free Space on File System (MB): 8,722

                  Archive Log Directory : e:\archlog
          Total Size of File System (MB): 603,751.82
          Used Space on File System (MB): 80,642.30
          Free Space on File System (MB): 523,109.52
                  Archive Log Compressed: Yes

                   Mirror Log Directory :
          Total Size of File System (MB):
          Used Space on File System (MB):
          Free Space on File System (MB):

        Archive Failover Log Directory :
          Total Size of File System (MB):
          Used Space on File System (MB):
          Free Space on File System (MB):
```

Field descriptions

Total Space
: Specifies the maximum size of the active log, in megabytes.

Used Space
: Specifies the amount of used active log space, in megabytes.

Free Space
: Specifies the amount of active log space that is not being used by uncommitted transactions, in megabytes.

Total Size of File System
: Specifies the total size of the file system, in megabytes.

Space Used on File System
: Specifies the amount of used space on the file system, in megabytes.

Free Space on File System
: Specifies the amount of space that is available on the file system, in megabytes.

Archive Log Compressed
: Specifies whether the archive logs are compressed.

Active Log Directory
: Specifies the location where active log files are stored. When you change the active log directory, the server moves all archived logs to the archive log directory and all active logs to a new active log directory.

Mirror Log Directory
: Specifies the location where the mirror for the active log is maintained.

Archive Failover Log Directory
: Specifies the location into which the server saves archive logs if the logs cannot be archived to the archive log directory.

Archive Log Directory
: Specifies the location into which the server can archive a log file after all the transactions that are represented in that log file are completed.

QUERY MACHINE (Query machine information)

Use this command to display information for one or more machines. You can use this information to recover IBM Spectrum Protect™ client machines in case of a disaster.

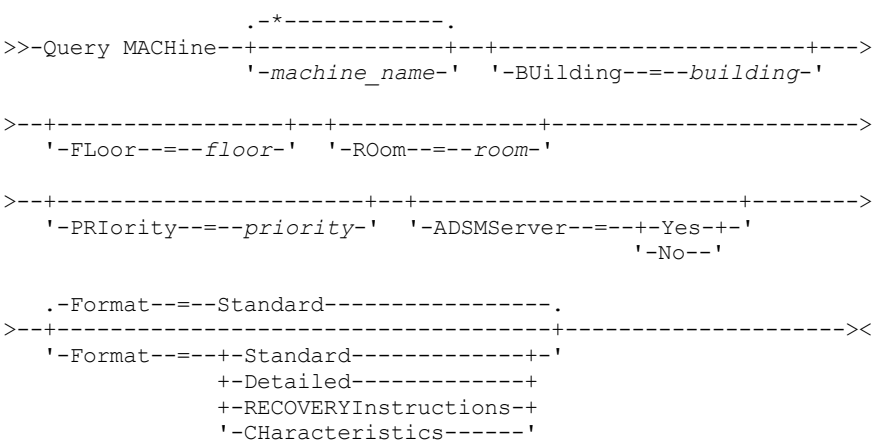
Attention: IBM Spectrum Protect does not use the information in any way. It is available only to help you plan for the disaster recovery of client machines.
IBM Spectrum Protect displays information for multiple machines in the following order:

- According to the priority specified.
- Within a priority, according to the specified location and machine name.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

machine_name
: Specifies the name of one or more machines to be queried. You can use wildcard characters to specify this name. This parameter is optional. The default is all machines that meet the specified criteria.

BUilding
: Specifies the name or number of the building that the machines are in. This parameter is optional. Enclose the text in quotation marks if it contains any blank characters.

FLoor
: Specifies the name or number of the floor that the machines are on. This parameter is optional. Enclose the text in quotation marks if it contains any blank characters.

ROom
: Specifies the name or number of the room that the machines are in. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters.

PRIority
: Specifies the priority number of the machines. This parameter is optional.

ADSMServer
: Specifies if the machine contains an IBM Spectrum Protect server. This parameter is optional. The default is to display any machines that meet the other criteria. Possible values are:

  Yes
  : The machine contains an IBM Spectrum Protect server.

  No
  : The machines do not contain an IBM Spectrum Protect server.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Displays partial information for the machines.

  Detailed
  : Displays all information for the machines.

  RECOVERYInstructions
  : Displays only machine recovery instructions. This option is valid only when querying a specific machine.

  CHaracteristics
  : Displays only machine characteristics. This option is valid only when querying a specific machine.

Example: Display information for a specific machine

Display information for a machine named MACH1. See Field descriptions for field descriptions.

```
query machine MACH1

Machine  Machine  Building Floor Room  Node Name  Recovery
Name     Priority                               Media Name
-------  -------- -------- ----- -----  ---------  ----------
MACH1       1       21       2   2929  VIRGINIA   RECMED1
```

Example: Display detailed information for priority 1 machines

Display detailed information for all priority 1 machines on the second floor of building 21. See Field descriptions for field descriptions.

```
query machine * building=21 floor=2 priority=1
format=detailed

                  Machine Name: MACH1
              Machine Priority: 1
                      Building: 21
                         Floor: 2
                          Room: 2929
                       Server?: Yes
                   Description: TSM server machine
                     Node Name: VIRGINIA
          Recovery Media Name: RECMED1
             Characteristics?: Yes
        Recovery Instructions?: Yes
```

Field descriptions

Machine Name
: The name of the machine.

Machine Priority
: The recovery priority of the machine.

Building
: The building in which the machine is located.

Floor
: The floor on which the machine is located.

Room
: The room in which the machine is located.

Server?
: Whether the machine contains an IBM Spectrum Protect server.

Description
: A description of the machine.

Node Name
: The IBM Spectrum Protect client nodes associated with this machine.

Recovery Media Name
: The recovery media associated with this machine.

Characteristics?
: Whether the characteristics text of the machine is stored in the database.

Recovery Instructions?
: Specifies whether recovery instructions text for a machine is stored in the IBM Spectrum Protect database.

Related commands

Table 1. Commands related to QUERY MACHINE

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
DEFINE MACHNODEASSOCIATION	Associates an IBM Spectrum Protect node with a machine.
DEFINE RECMEDMACHASSOCIATION	Associates recovery media with a machine.
DELETE MACHINE	Deletes a machine.
INSERT MACHINE	Inserts machine characteristics or recovery instructions into the IBM Spectrum Protect database.
UPDATE MACHINE	Changes the information for a machine.

QUERY MEDIA (Query sequential-access storage pool media)

Use this command to display information about the sequential-access primary and copy storage pool volumes moved by the MOVE MEDIA command.

Privilege class

Any administrator with system or operator privilege can issue this command unless it includes the CMD parameter. If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have operator, unrestricted storage, or system privilege. If the CMD parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES (the default), the administrator must have system privilege.

The QUERY MEDIA command displays only volumes with an ACCESS MODE value of READONLY or READWRITE.

Syntax

```
                .-*-----------.
>>-Query MEDia--+-------------+--STGpool--=--pool_name----------><
                '-volume_name-'
```

Parameters

volume_name
: Specifies the name of the sequential-access primary or copy storage pool volume to display. This parameter is optional. You can use a wildcard character to specify the name. All matching volumes are considered for processing. If you do not specify this parameter, all volumes defined in the storage pool specified with the STGPOOL parameter display.

STGpool (Required)
: Specifies the name of the sequential-access primary or copy storage pool that is used to select the volumes for processing. You can use wildcard characters to specify the name. All matching storage pools are processed. If the storage pool specified is not managed by an automated library, no volumes display.

Days
: Specifies the number of days that must elapse, after the volume has been written to or read from, before the volume is eligible for processing. This parameter is optional. You can specify a number from 0 to 9999. The default value is 0. The most recent of the volume's last written date or last read date is used to calculate the number of days elapsed.

WHERESTATUs
: Specifies that the output of the query should be restricted by volume status. This parameter is optional. You can specify more than one status in a list by separating each status with a comma and no intervening spaces. If you do not specify a value for this parameter, all volumes in the specified storage pool, regardless of their status, are displayed.

  Possible values are:

  FULl
  : Specifies that volumes with a status of FULL display.

  FILling
  : Specifies that volumes with a status of FILLING display.

  EMPty
  : Specifies that volumes with a status of EMPTY display.

WHEREACCess
: Specifies that output should be restricted by volume access mode. This parameter is optional. If you do not specify a value for this parameter, output is not restricted by access mode.

  Possible values are:

  READWrite
  : Specifies that volumes with an access mode of READWRITE display.

READOnly
Specifies that volumes with an access mode of READONLY display.

Format
Specifies how information displays. This parameter is optional. The default value is STANDARD. Possible values are:

Standard
Specifies that partial information displays for the specified sequential access storage pool volumes.
Detailed
Specifies that complete information displays for the specified sequential access storage pool volumes.
Cmd
Specifies that executable commands are built for the storage pool volumes processed by the QUERY MEDIA command. These commands will be in the file specified with the CMDFILENAME parameter on the QUERY MEDIA command. If you want the commands to display on the console only, specify a null string ("") for the CMDFILENAME. If FORMAT=CMD is specified but no command string is specified with the CMD parameter, the QUERY MEDIA command will fail.

WHERESTate
Specifies the state of volumes to process. This parameter restricts processing to volumes that have the specified state. This parameter is optional. The default is ALL. Possible values are:

All
Specifies that volumes in all states are queried. The valid states are: MOUNTABLEINLIB and MOUNTABLENOTINLIB.
MOUNTABLEInlib
Specifies that volumes that are currently in the MOUNTABLEINLIB state are queried. Volumes in the MOUNTABLEINLIB state are in the library, and are onsite, contain valid data, and are available for onsite processing.
MOUNTABLENotinlib
Specifies that volumes that are currently in the MOUNTABLENOTINLIB state are queried. Volumes in the MOUNTABLENOTINLIB state are not in the library, do not contain valid data, and are not available for onsite processing.

WHEREOVFLOcation
Specifies the overflow location of the volumes to display. This parameter is optional. This parameter restricts processing to volumes that are in the specified location. The maximum length of the location is 255 characters. The location must be enclosed in quotation marks if it contains any blank characters.

CMd
Specifies the creation of executable commands. Enclose the command specification in quotation marks. The maximum length of the command specification is 255 characters. This parameter is optional.

For each volume successfully processed by the QUERY MEDIA command, the server writes the associated commands to a file. Specify the file name with the CMDFILENAME parameter.

AIX Linux If you do not specify a filename, the command will generate a default filename by appending the string exec.cmds.media to the server directory.

Windows If you do not specify a filename, the command will generate a default filename by appending the string exec.cmd.media to the server directory.

Remember:

1. If the command written to the file exceeds 255 characters, it is split into multiple lines, and a continuation character (+) is added to all but the last line. You may need to alter the continuation character according to the requirements of the product that runs the commands.
2. If an executable command is specified with any value for FORMAT other than CMD, the command string is ignored, and the QUERY MEDIA command will not write any command line.

Specify a command string and any substitution variables:

string
Specifies the string to build an executable command to process the volume name or volume location or both. You can specify any free form text for the string. Do not use embedded quotation marks. For example, the following is a valid executable command specification:

```
cmd="checkin libvolume &vol"
```

The following is an invalid executable command specification:

```
cmd="checkin libvolume "&vol""
```

substitution
: Specifies a variable for which you want the QUERY MEDIA command to substitute a value. The possible substitution variables are:

  &VOL
  : Substitute the volume name for &VOL. You can specify lowercase characters, &vol. No spaces or blanks are allowed between ampersand, &, and VOL. If there are spaces or blanks between ampersand and VOL, the QUERY MEDIA command will treat them as strings and no substitution will be set. If &VOL is not specified, no volume name is set in the executable command.

  &LOC
  : Substitute the volume location for &LOC. You can specify lowercase characters, &loc. No spaces or blanks are allowed between ampersand, &, and LOC. If there are spaces or blanks between ampersand and LOC, the QUERY MEDIA command will treat them as strings and no substitution will be set. If &LOC is not specified, no location name is set in the executable command.

  &VOLDSN
  : Substitute the volume file name for &VOLDSN. An example of a copy storage pool tape volume file name using the defined prefix IBM Spectrum Protect™310 is IBM Spectrum Protect310.BFS. If &VOLDSN is not specified, no volume file name is set in the executable command.

  &NL
  : Substitute the new line character for &NL. When &NL is specified, the QUERY MEDIA command will split the command at the position where the &NL is and will not append any continuation character. The user is responsible for specifying the proper continuation character before the &NL if one is required. The user is also responsible for the length of the line written. If the &NL is not specified and the command exceeds 255 characters, the command is split into multiple lines, and a continuation character (+) is added to all but the last line.

CMDFilename
: Specifies the full path name that will contain the commands specified with CMD parameter when FORMAT=CMD is specified. This parameter is optional. The maximum length of the file name is 1279 characters.

  AIX Linux If you specify "" with the CMDFILENAME parameter, the QUERY MEDIA command will generate a file name by appending the "exec.cmds.media" to the server directory. The server directory is the current working directory of the server process.

  Windows If you specify "" with the CMDFILENAME parameter, the QUERY MEDIA command will generate a file name by appending the "exec.cmd.media" to the server directory. The server directory is the current working directory of the server process.

  If you specify a null string ("") for the CMDFILENAME, the commands built are displayed on the console only. You can redirect the commands displayed to a file by using the redirection characters for the operating system (> or >>).

  AIX Linux If the filename is not specified, the command will generate a default filename by appending the string "exec.cmds.media" to the server directory.

  Windows If the filename is not specified, the command will generate a default filename by appending the string "exec.cmd.media" to the server directory.

  The QUERY MEDIA command automatically allocates the file name specified or generated. If the file name exists, the QUERY MEDIA command will attempt to use it and the existing data, if any, in the file to be overwritten. You can specify APPEND=YES to prevent the existing data from being overwritten. If the QUERY MEDIA command fails after the command file is allocated, the file is not deleted.

APPend
: Specifies to write at the beginning or the ending of the command file data. This parameter is optional. The default is NO. Possible values are:

  No
  : Specifies to write the data from the beginning of the command file. If the given command file exists, its contents are overwritten.

  Yes
  : Specifies to append the command file by writing at the end of the command file data.

Example: Display information on a specific sequential access storage pool

Display all full and partial full volumes that are in the sequential access primary storage pool, ARCHIVE. See Field descriptions for field descriptions.

```
query media * stgpool=archive wherestatus=full, filling


Volume Name State                Location             Automated
                                                      LibName
----------- -------------------  -------------------- -----------
TAPE01      Mountable in Library                      LIB3494
TAPE03      Mountable not in Lib. Room1234/Bldg31
TAPE07      Mountable in Library                      LIB3494
TAPE09      Mountable not in Lib. Room1234/Bldg31
```

Example: Display information on sequential access storage pool with a specific prefix

Display in detail all full volumes in MOUNTABLENOTINLIB state for sequential access storage pools that have a prefix name of ONSITE. See Field descriptions for field descriptions.

```
query media wherestate=mountablenotinlib stgpool=onsite*
wherestatus=full format=detailed

      Volume Name: TAPE21
                  State: Mountable not in library
          Volume Status: Full
                 Access: ReadOnly
    Last Reference Date: 01/30/98
  Last Update Date/Time: 08/20/1996 13:29:02
               Location: Rm569/bldg31
      Storage Pool Name: ONSITE.ARCHIVE
      Automated Libname:

            Volume Name: TAPE22
                  State: Mountable not in library
          Volume Status: Full
                 Access: ReadOnly
    Last Reference Date: 01/30/98
  Last Update Date/Time: 08/20/1996 15:29:02
               Location: Rm569/bldg31
      Storage Pool Name: ONSITE.ARCHIVEPOOL
      Automated Libname:
```

Example: Generate checkin commands

Generate the CHECKIN LIBVOLUME commands for full and partially full volumes that are in the ONSITE.ARCHIVE primary storage pool and stored in the overflow location Room 2948/Bldg31.

```
query media * stgpool=onsite.archive format=cmd
wherestatus=full,filling wherestate=mountablenotinlib
whereovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

The QUERY MEDIA command created the CHECKIN LIBVOLUME executable commands in /tsm/move/media/checkin.vols, which can be run by issuing the MACRO command with /tsm/move/media/checkin.vols as the macro name.

```
checkin libvol lib3494 TAPE04 status=private
checkin libvol lib3494 TAPE13 status=private
checkin libvol lib3494 TAPE14 status=private
```

Field descriptions

Volume Name
: Specifies the name of the primary sequential access storage pool volume.

State
: Specifies the state of the volume.

Volume Status
: Specifies the status of the volume.

Access
: Specifies the access mode of the volume.

Last Reference Date
: Specifies the volume's last written date or last read date, whichever is more recent.

Last Update Date/Time
: Specifies the date and time when the volume was most recently updated.

Location
: Specifies where the volume is stored. If the volume is ejected from the library and its location is not specified or defined, a question mark (?) is displayed for the location.

Storage Pool Name
: Specifies the name of the sequential access storage pool where the volume is defined.

Automated LibName
: Specifies the automated library name if the volume is in the library.

Related commands

Table 1. Commands related to QUERY MEDIA

Command	Description
AIX Linux Windows MOVE MEDIA	Moves storage pool volumes that are managed by an automated library.

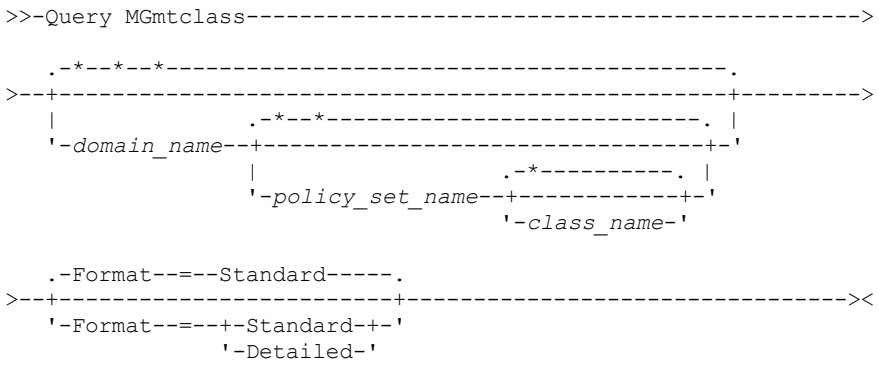
QUERY MGMTCLASS (Query a management class)

Use this command to display information about management classes.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

domain_name
: Specifies the policy domain associated with the management class to query. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, management classes in all policy domains are queried. You must specify this parameter when querying an explicitly named management class.

policy_set_name
: Specifies the policy set associated with the management class to query. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, management classes in all policy sets are queried. You must specify this parameter when querying an explicitly named management class.

class_name
: Specifies the management class to query. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, all management classes are queried.

Format

Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

Standard
: Specifies that partial information is displayed.

Detailed
: Specifies that complete information is displayed.

Example: Display information for all management classes

Query all management classes for all policy domains. Create the output in standard format. See Field descriptions for field descriptions.

```
query mgmtclass

Policy       Policy       Mgmt         Default     Description
Domain       Set Name     Class        Mgmt
Name                      Name         Class ?
---------    ---------    ---------    ---------   ------------------
EMPLOYEE-    ACTIVE       ACTIVEFI-    Yes         Modified default
 _RECORDS                  LES                      management class
EMPLOYEE-    HOLIDAY      ACTIVEFI-    Yes         Modified default
 _RECORDS                  LES                      management class
EMPLOYEE-    HOLIDAY      FILEHIST-    No          Test modified
 _RECORDS                  ORY                      management class
EMPLOYEE-    VACATION     ACTIVEFI-    Yes         Original default
 _RECORDS                  LES                      management class
EMPLOYEE-    VACATION     FILEHIST-    No          Test modified
 _RECORDS                  ORY                      management class
PROG1        SUMMER       MCLASS1      No          Technical Support
                                                    Mgmt Class
PROG2        SUMMER       MCLASS1      No          Technical Support
                                                    Mgmt Class
STANDARD     ACTIVE       STANDARD     Yes         Installed default
                                                    management class
STANDARD     STANDARD     STANDARD     Yes         Installed default
                                                    management class
```

To display information about management classes in a specific policy domain, for example the domain ENGPOLDOM, issue the following command:

```
query mgmtclass engpoldom * *
```

Example: Display detailed information for a specific management class

Query the ACTIVEFILES management class that is assigned to the VACATION policy set of the EMPLOYEE_RECORDS policy domain. Create the output in detailed format. See Field descriptions for field descriptions.

```
query mgmtclass employee_records vacation
activefiles format=detailed

             Policy Domain Name: EMPLOYEE_RECORDS
                Policy Set Name: VACATION
                Mgmt Class Name: ACTIVEFILES
          Default Mgmt Class ?: Yes
                    Description: Installed default management class
     Space Management Technique: None
        Auto-Migrate on Non-Use: 0
     Migration Requires Backup?: Yes
          Migration Destination: SPACEMGPOOL
 Last Update by (administrator): $$CONFIG_MANAGER$$
          Last Update Date/Time: 05/31/1998 13:15:45
               Managing Profile: EMPLOYEE
                Changes Pending: Yes
```

Field descriptions

Policy Domain Name
: The policy domain.

Policy Set Name
: The policy set.

Mgmt Class Name
: The management class.

Default Mgmt Class ?
: Whether the management class is the default management class for the policy set.

Description
: The description of the management class.

Space Management Technique
: The space management technique for the management class, for IBM Spectrum Protect™ for Space Management clients.

Auto-Migrate on Non-Use
: The number of days that must elapse since a file was last accessed before it is eligible for automatic migration by IBM Spectrum Protect for Space Management clients.

Migration Requires Backup?
: Whether a backup version of a file must exist before a file can be migrated by IBM Spectrum Protect for Space Management clients.

Migration Destination
: The storage pool that is the destination for files migrated by IBM Spectrum Protect for Space Management clients.

Last Update by (administrator)
: The administrator or server that most recently updated the management class. If this field contains $$CONFIG_MANAGER$$, the management class is associated with a domain that is managed by the configuration manager.

Last Update Date/Time
: The date and time when the management class was most recently defined or updated.

Managing profile
: The profile or profiles to which the managed server subscribed to get the definition of this management class.

Changes Pending
: Whether or not changes are being made but not activated. Once the changes are activated, the field resets to No.

Related commands

Table 1. Commands related to QUERY MGMTCLASS

Command	Description
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE MGMTCLASS	Defines a management class.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY DOMAIN	Displays information about policy domains.
UPDATE MGMTCLASS	Changes the attributes of a management class.

QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)

Use this command to display information about alert monitoring and server status settings.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query MONITORSEttings---------------------------------------><
```

Display monitoring settings

Display details about the monitoring settings. See Field descriptions for more details.

```
query monitorsettings
```

Example output:

```
                            Monitor Status: On
            Status Refresh Interval (Minutes): 5
                     Status Retention (Hours): 48
                       Monitor Message Alerts: On
              Alert Update Interval (Minutes): 10
                            Alert to Email: On
         Send Alert Summary to Administrators: On
                     Alert from Email Address: DJADMIN@MYDOMAIN.COM
                              Alert SMTP Host: DJHOST.MYDOMAIN.COM
                              Alert SMTP Port: 25
              Alert Active Duration (Minutes): 480
            Alert Inactive Duration (Minutes): 480
              Alert Closed Duration (Minutes): 60
                             Monitoring Admin: ADMIN
                              Monitored Group: MONGROUP
                            Monitored Servers: SERVER2
           At-Risk Interval for Applications: 24
    Skipped files as At-Risk for Applications?: Yes
         At-Risk Interval for Virtual Machines: 24
Skipped files as At-Risk for Virtual Machines?: Yes
                 At-Risk Interval for Systems: 24
         Skipped files as At-Risk for Systems?: Yes
                         Deployment Repository: /source/packages/deploy
                  Maximum Deployment Packages: 4
                   Deployment Package Manager: On
```

Field descriptions

Monitor Status
: Specifies whether alert monitoring on the server is enabled or disabled.

Status Refresh Interval (Minutes)
: Specifies the number of minutes between intervals that the monitoring server gathers event data.

Status Retention (Hours)
: Specifies the number of hours that status monitoring indicators are retained.

Monitor Message Alerts
: Specifies whether alerts are sent to administrators by email.

Alert Update Interval (Minutes)
: Specifies the length of time, in minutes, that the alert monitor waits before the alert is updated and pruned on the server.

Alert to Email
: Specifies whether alerts are sent to administrators by email.

Send Alert Summary to Administrators
: Specifies the administrators that receive a summary of existing alerts on the server in an email.

Alert from Email Address
: Specifies the email address of the sender.

Alert SMTP Host
: Specifies the Simple Mail Transfer Protocol (SMTP) host mail server that is used to send alerts by email.

Alert SMTP Port
: Specifies the SMTP mail server port that is used to send alerts by email.

Alert Active Duration (Minutes)
: Specifies how long, in minutes, an alert remains active.

Alert Inactive Duration (Minutes)
: Specifies how long, in minutes, an alert remains inactive.

Alert Closed Duration (Minutes)
: Specifies how long, in minutes, an alert remains closed before it is deleted from the server.

Monitoring Admin
: Specifies the name of the monitoring administrator that is used to connect to the servers in the monitored group.

Monitored Group
: Specifies the name of the monitored server group.

Monitored Servers
: Specifies the names of the servers in the monitored server group. The monitor settings might be different on each monitored server. If so, issue the query command for each server to display the monitoring settings.

At-Risk Interval for Applications

Specifies how long, in hours, an applications client can log no activity before it is considered at-risk.

Skipped files as At-Risk for Applications?

Specifies that the server considers skipped files, by the client as a failure, and marks the client at-risk.

At-Risk Interval for Virtual Machines

Specifies how long, in hours, a virtual client can log no activity before it is considered at-risk.

Skipped files as At-Risk for Virtual Machines?

Specifies that the server considers skipped files, by the client as a failure and marks the client at-risk.

At-Risk Interval for Systems

Specifies how long, in hours, a systems client can log no activity before it is considered at-risk.

Skipped files as At-Risk for Systems?

Specifies that the server considers skipped files, by the client as a failure, and marks the client at-risk.

Deployment Repository

Specifies the location where client deployment packages are downloaded, and the location of the storage volumes that are used for client deployment packages.

Maximum Deployment Packages

Specifies the maximum number of client deployment packages that are stored in the deployment repository for each product version.

Deployment Package Manager

Specifies whether the deployment package manager queries the FTP site for new deployment packages and downloads new packages as they become available.

Related commands

Table 1. Commands related to QUERY MONITORSETTINGS

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
DELETE GRPMEMBER (Delete a server from a server group)	Deletes a server from a server group.
DELETE SERVER (Delete a server definition)	Deletes the definition of a server.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
SET ALERTMONITOR (Set the alert monitor to on or off)	Specifies whether alert monitoring is set to on or off.
SET DEPLOYREPOSITORY (Set the download path for client deployment packages)	Specifies the location where client deployment packages are downloaded.
SET DEPLOYMAXPKGS (Set the maximum number of client deployment packages to store)	Specifies the maximum number of client deployment packages that are downloaded and stored on the server.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

QUERY MONITORSTATUS (Query the monitoring status)

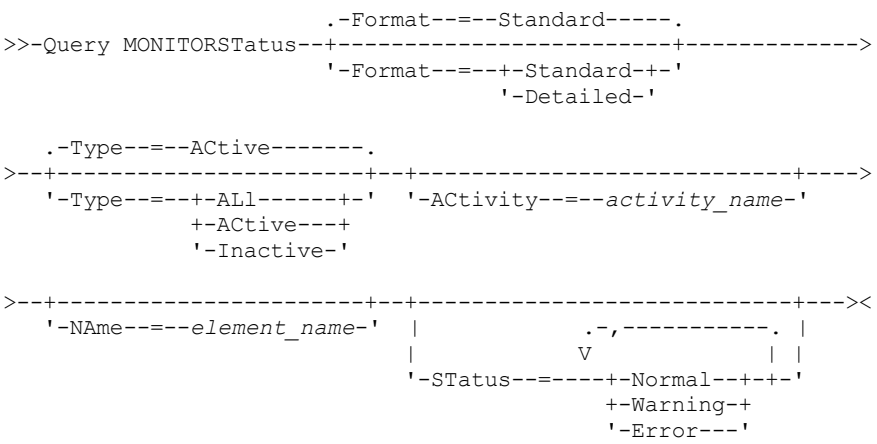
Use this command to display monitoring messages that are within the defined status retention period.

You can limit the output to a specified status, such as only messages with a status of active. If you do not specify any parameters, all messages are displayed.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

Format
: Specifies the amount of information that is displayed. The default value is STANDARD. Specify one of the following values:

  Standard
  : Specifies that only partial information is displayed for the specified messages.

  Detailed
  : Specifies that all information is displayed for the specified messages.

Type
: This parameter restricts the output to only messages with the specified type value. Specify one of the following values:

  ALl
  : Displays all information.

  ACtive
  : Displays all active messages. This is the default value.

  Inactive
  : Displays all inactive messages.

ACtivity
: Specifies the activity that you want to query. See the DEFINE STATUSTHRESHOLD command for details on available activities to query.

NAme
: Specifies the name that you want to query. The NAME value refers to the name of the element with the specified activity. For example, a status indicator that contains information about a storage pool that is called `backuppool` has the NAME set to BACKUPPOOL.

STatus
: Specifies the status of the messages that you want to query. You can specify multiple status values in a list by separating the values with commas and no intervening spaces. If you do not specify a value for this parameter, information for all status values is displayed. Specify one of the following values:

  Normal
  : Displays all messages with a normal status.

  Warning
  : Displays all messages with a warning status.

  Error
  : Displays all messages with an error status.

Display monitoring settings

Display details about the monitoring status.

```
Query MONITORStatus type=active
```

Example output:

```
          Server Name: SERVER1
        Activity Date: 03/05/2013 15:57:37
        Activity Name: CAPACITY OF PRIMARY DISK AND FILE STORAGE
         Element Name: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Element Numeric Value: 0
 Element String Value:
        Element State: NORMAL

          Server Name: SERVER1
        Activity Date: 03/05/2013 15:57:37
        Activity Name: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
         Element Name: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Element Numeric Value: 0
 Element String Value:
        Element State: NORMAL

          Server Name: SERVER1
        Activity Date: 03/05/2013 15:57:37
        Activity Name: CAPACITY OF PRIMARY TAPE STORAGE
         Element Name: CAPACITY OF PRIMARY TAPE STORAGE
Element Numeric Value: 0
 Element String Value:
        Element State: NORMAL

          Server Name: SERVER1
        Activity Date: 03/05/2013 15:57:37
        Activity Name: USED CAPACITY OF PRIMARY TAPE STORAGE
         Element Name: USED CAPACITY OF PRIMARY TAPE STORAGE
Element Numeric Value: 0
 Element String Value:
        Element State: NORMAL
```

Display monitoring settings

Display details about the monitoring status.

```
query monitorstatus f=d type=active
```

Example output:

```
                      Server Name: SERVER1
                    Activity Date: 03/05/2013 15:57:37
                    Activity Name: CAPACITY OF PRIMARY DISK AND
                                   FILE STORAGE
                     Element Name: CAPACITY OF PRIMARY DISK AND
                                   FILE STORAGE
            Element Numeric Value: 0
             Element String Value:
                    Element State: NORMAL
                  Element Details:
         Primary Repair Suggestion:
 First Alternate Repair Suggestion:
Second Alternate Repair Suggestion:

                      Server Name: SERVER1
                    Activity Date: 03/05/2013 15:57:37
                    Activity Name: USED CAPACITY OF PRIMARY DISK AND
                                   FILE STORAGE
                     Element Name: USED CAPACITY OF PRIMARY DISK AND
                                   FILE STORAGE
            Element Numeric Value: 0
             Element String Value:
                    Element State: NORMAL
                  Element Details:
         Primary Repair Suggestion:
 First Alternate Repair Suggestion:
```

```
Second Alternate Repair Suggestion:

                      Server Name: SERVER1
                    Activity Date: 03/05/2013 15:57:37
                    Activity Name: CAPACITY OF PRIMARY TAPE STORAGE
                     Element Name: CAPACITY OF PRIMARY TAPE STORAGE
             Element Numeric Value: 0
              Element String Value:
                     Element State: NORMAL
                   Element Details:
         Primary Repair Suggestion:
 First Alternate Repair Suggestion:
Second Alternate Repair Suggestion:

                      Server Name: SERVER1
                    Activity Date: 03/05/2013 15:57:37
                    Activity Name: USED CAPACITY OF PRIMARY
                                   TAPE STORAGE
                     Element Name: USED CAPACITY OF PRIMARY
                                   TAPE STORAGE
             Element Numeric Value: 0
              Element String Value:
                     Element State: NORMAL
                   Element Details:
         Primary Repair Suggestion:
 First Alternate Repair Suggestion:
Second Alternate Repair Suggestion:
```

Field descriptions

Server Name
: The name of the server.

Activity Date
: The last date and time activity was reported.

Activity Name
: The name of the activity.

Element Name
: The name of the element.

Element Numeric Value
: The numeric value of the element.

Element String Value
: The string value of the element.

Element State
: The state of the element.

Element Details
: The detailed information of the element.

Primary Repair Suggestion
: The primary repair suggestion.

First Alternate Repair Suggestion
: The repair suggestion to follow if the primary suggestion is not adequate.

Second Alternate Repair Suggestion
: The repair suggestion to follow if the primary and first alternate suggestions are not adequate.

Related commands

Table 1. Commands related to QUERY MONITORSTATUS

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.

Command	Description
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

QUERY MOUNT (Display information on mounted sequential access volumes)

Use this command to display information about the status of one or more sequential access volumes that are mounted.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-*-----------.  .-Format--=--Standard-----.
>>-Query MOunt--+-------------+--+-------------------------+---><
                '-volume_name-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'
```

Parameters

volume_name
: Specifies the name of the mounted sequential access volume. You can use wildcard characters to specify this name. This parameter is optional. The default is all mounted volumes.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: List all mounted sequential volumes

Display information on all mounted sequential media volumes.

```
query mount
```

AIX

```
ANR8330I 3590 volume D6W992 is mounted R/O
in drive RMT1(/dev/rmt1), status: IN USE.
ANR8334I  1 volumes found.
ANR8331I 8MMTAPE volume WPD000 is mounted R/W
in drive 8MM.1 (/dev/mt0), status: DISMOUNTING.
ANR8334I  1 volumes found.
```

Linux

```
ANR8330I 3590 volume D6W992 is mounted R/O
in drive RMT1/dev/IBMtape1, status: IN USE.
ANR8334I  1 volumes found.
ANR8331I 8MMTAPE volume WPD000 is mounted R/W
in drive 8MM.1 (/dev/tsmscsi/mt0), status: DISMOUNTING.
ANR8334I  1 volumes found.
```

Windows

```
ANR8330I 3590 volume D6W992 is mounted R/O
in drive RMT1(/dev/rmt1), status: IN USE.
ANR8334I  1 volumes found.
ANR8331I 8MMTAPE volume WPD000 is mounted R/W
in drive 8MM.1 (mt3.0.0.0), status: DISMOUNTING.
ANR8334I  1 volumes found.
```

Remember:

1. If the status of a volume is full or if its access mode is read-only (R/O), the mount mode of the volume is R/O. To determine the status and access mode of a volume, issue the QUERY VOLUME FORMAT=DETAILED command. If a volume can be written to (that is, the status is filling or empty), the mount mode of the volume is read/write (R/W), even if it is only being read.
2. In a storage pool that is associated with the FILE or CENTERA device type, the server can complete concurrent multiple read-access and one write-access to the same volume. As a result, a volume in a storage pool with a device type of FILE or CENTERA can appear to be mounted more than once.
3. In the message ANR8448I, the drive name is listed as `UNKNOWN` for volumes of the FILE device type with a non-shared device class. The reason is that no drive is associated with the volumes; drive names are shown in the file-based library.
4. If you issue the QUERY MOUNT command while the drive is being cleaned, the command output continues to show a `DISMOUNTING` status for the dismounted volume until the cleaning completes.

Example: Display detailed information about mounted sequential volumes

Display details about mounted volumes.

```
query mount format=detailed
```

```
ANR2017I Administrator SERVER_CONSOLE issued command: QUERY
MOUNT format=detailed
ANR8487I Mount point in device class FILE is waiting for the
volume mount to
complete -- owning server: SERVER1, status: WAITING FOR VOLUME
(session: 0, process: 1).
ANR8488I LTO volume 015005L4 is mounted R/W in drive IBMVTL1
(/dev/rmt37) -- owning
server: SERVER1, status: IN USE (session: 0, process: 2).
ANR8486I Mount point in device class FILE is reserved -- owning
server: SERVER1,
status: RESERVED (session: 5, process: 0).
ANR8334I         3 matches found.
```

Related commands

Table 1. Commands related to QUERY MOUNT

Command	Description
DISMOUNT VOLUME	Dismounts a sequential, removable volume by the volume name.
REPLY	Allows a request to continue processing.

QUERY NASBACKUP (Query NAS backup images)

Use this command to display information about the file system image objects that have been backed up for a specific NAS node and file space. You can only use this command to display objects that were backed up for a NAS node using NDMP.

The server displays all matching objects, the dates that these objects were backed up, and information about a table of contents (TOC) for the object.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query NASBAckup--node_name--filespace_name------------------->

   .-BEGINDate--=--TODAY - 7-.  .-BEGINTime--=--00:00:00-.
>--+-------------------------+--+----------------------+------>
   '-BEGINDate--=--date------'  '-BEGINTime--=--time-----'

   .-ENDDate--=--TODAY-.  .-ENDTime--=--23:59:59-.
>--+-------------------+--+---------------------+-------------->
   '-ENDDate--=--date--'  '-ENDTime--=--time-----'

   .-TYPE--=--BACKUPImage-----.
>--+-------------------------+------------------------------><
   '-TYPE--=--+-BACKUPImage-+-'
              '-SNAPMirror--'
```

Parameters

node_name (Required)
: Specifies the name of the NAS node for which backup objects are displayed. You cannot use wildcards to specify this name.

filespace_name (Required)
: Specifies the name of the file space for which backup objects are displayed. You can use wildcards to specify this name.

BEGINDate
: Specifies the beginning date to select the backup objects to display. All backup objects that were created on or after the specified date are displayed. The default is seven days prior to the current date. You can use this parameter with the BEGINTIME parameter to specify a range for the date and time. This parameter is optional.
You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/2002
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY –7 *or* –7. To display information about the image objects that have been created a week ago, you can specify BEGINDATE=TODAY-7 or BEGINDATE= -7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime
: Specifies the beginning time to select the backup objects to display. All backup objects created on or after the specified time display. This parameter is optional. The default is midnight (00:00:00) on the date specified for the BEGINDATE.
You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	10:30:08
NOW	The current time on the specified begin date	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with BEGINTIME=NOW+3 or BEGINTIME=+3, the server displays image objects with a time of 12:00 or later on the begin date.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-04:00 *or* -04:00. If you issue this command at 9:00 with BEGINTime=NOW-3:30 or BEGINTime= -3:30, the server displays image objects with a time of 5:30 or later on the begin date.

ENDDate

Specifies the ending date used to select the backup objects to be displayed. All backup objects created on or before the specified date are displayed. This parameter is optional. The default is the current date. You can use this parameter with the ENDTIME parameter to specify an ending date and time.

You can specify the date using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/2002
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified. The maximum number of days you can specify is 9999.	TODAY–1 *or* –1. To display information created up to yesterday, you can specify ENDDATE=TODAY-1 or simply ENDDATE= -1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time used to select the backup objects to be displayed. All backup objects created on or before the specified time are displayed. This parameter is optional. The default is 23:59:59. You can use this parameter with the ENDDATE parameter to specify a range for the date and time.

You can specify the time using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW

Value	Description	Example
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 *or* +03:00. If you issue this command at 9:00 with ENDTIME=NOW+3:00 or ENDTIME= +3:00, the server displays image objects with a time of 12:00 or later on the end date you specify.
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified end date	NOW-03:30 *or* -03:30. If you issue this command at 9:00 with ENDTIME=NOW-3:30 or ENDTIME= -3:30, the server displays image objects with a time of 5:30 or later on the end date you specify.

TYPE

Specifies the type of NDMP backup images for which you want to display information. The default value for this parameter is BACKUPIMAGE. Other image types represent backup methods that might be specific to a particular file server. Possible values are:

BACKUPImage
: Specifies that the output should show only the standard NAS base and differential images. This is the default value for this parameter.

SNAPMirror
: Specifies whether to display information about NetApp SnapMirror images. SnapMirror images are block-level full-backup images of a file system. A SnapMirror image can only be restored to a file system that has been prepared as a SnapMirror target volume. Refer to the documentation that came with your NetApp file server for more information. This parameter is valid for NetApp and IBM N-Series file servers only.

Example:

Issue the QUERY NASBACKUP command to display information about a node, nas1, and a filespace, /vol/vol1.

```
query nasbackup nas1 /vol/vol1

Node  Filespace Object      Object  Creation   Has       Mgmt      Image
Name  Name      Type        Size    Date       Table of  Class     Storage
                (MB)        (MB)    Contents   Contents  Name      Pool
                                               (TOC)               Name
----- --------  ---------   -----   ---------- --------  --------  --------
NAS1  vol/vol1  Full image  1050.5  10/22/2002  YES       DEFAULT   NASBACKUPS
                                     10:50:57
NAS1  vol/vol1  Differential  9.1   10/22/2002  YES       DEFAULT   NASBACKUPS
                image                 11:03:21
NAS1  vol/vol1  Full image  1050.5  10/22/2006  YES       STANDARD  FILEPOOL
                                     10:43:00
NAS1  vol/vol1  Differential  9.1   10/25/2006  YES       STANDARD  FILEPOOL
                image                 11:53:21
```

Example:

Issue the QUERY NASBACKUP command to display information about all NetApp SnapMirror to Tape images for a node, nas2, and a filespace, /vol/vol2.

```
query nasbackup nas2 /vol/vol2 type=snapmirror

Node  Filespace Object      Object  Creation    Mgmt Class  Image
Name  Name      Type        Size    Date        Name        Storage
                            (MB)                            Pool Name
----- --------  ----------  ------  ----------  ---------   ---------
NAS2  vol/vol2  SnapMirror  1050.5  04/02/2008  STANDARD    MYPOOL
                                     10:50:57
NAS2  vol/vol2  SnapMirror  1450.5  04/02/2008  STANDARD    MYPOOL
                                     11:03:21
```

Field descriptions

Node Name
: The name of the client node.

Filespace Name
: The name of the filespace.

Object Type
: The type of object backed up.

Object Size (MB)
: The size of the object in megabytes.

Creation Date
: The date the backup was created.

Mgmt Class Name
: The name of the management class.

Image Storage Pool Name
: The name of the storage where the backup resides.

Related commands

Table 1. Commands related to QUERY NASBACKUP

Command	Description
BACKUP NODE	Backs up a network-attached storage (NAS) node.
BACKUP NAS (IBM Spectrum Protect™ client command)	Creates a backup of NAS node data.
QUERY TOC	Displays details about the table of contents for a specified backup image.
RESTORE NODE	Restores a network-attached storage (NAS) node.

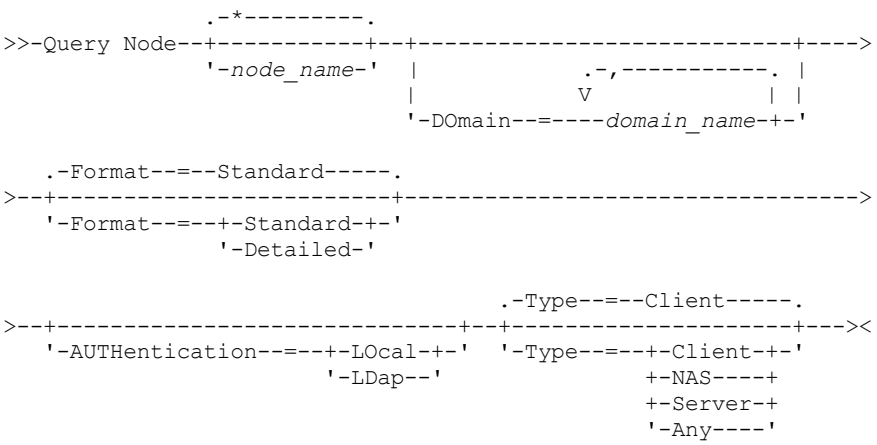
QUERY NODE (Query nodes)

Use this command to view information about one or more registered nodes.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

node_name
: Specifies the name of the client node to be queried. You can use wildcard characters to specify this name. All matching client nodes are queried. If you do not specify a value for this parameter, all client nodes are queried. The parameter is optional.

DOmain
: Specifies a list of policy domains that limit the client node query. Only nodes that are assigned to one of the specified policy domains are displayed. This parameter is optional. Separate the items in the list by commas, with no intervening spaces. You can use wildcard characters to specify a domain. All clients that are assigned to a matching domain are displayed. If you do not specify a value for this parameter, all policy domains are included in the query.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. You can specify one of the following values:

  Standard
  : Specifies that partial information is displayed for the specified client nodes.

  Detailed
  : Specifies that complete information is displayed for the specified client nodes.

Type
: Specifies the type of node to include in the query results. The parameter is optional. The default value is CLIENT. You can specify one of the following values:

  Any
  : Specifies any type of node.

  Client
  : Specifies client nodes that are backup-archive clients, IBM Spectrum Protect™ for Space Management clients, or application clients.

  NAS
  : Specifies NAS nodes.

  Server
  : Specifies client nodes that are other servers.

Authentication
: Specifies the password authentication method for the node.

  LOcal
  : Display those nodes that authenticate to the IBM Spectrum Protect server.

  LDap
  : Display those nodes that authenticate to an LDAP directory server. The node password is case-sensitive.

Example: Display information about registered client nodes

Display information about all registered client nodes.

```
query node
```

```
Node Name    Platform  Policy Domain  Days Since  Days Since  Locked?
                       Name                Last    Password
                                       Access         Set
---------    --------  --------       ---------   ---------- -------
CLIENT1      AIX       STANDARD              6            6    No
GEORGE       AIX       STANDARD              1            1    No
JANET        AIX       STANDARD              1            1    No
JARED        Linux86   STANDARD              1            1    No
JOE2         Mac       STANDARD             <1           <1    No
TOMC         WinNT     STANDARD              1            1    No
```

Example: Displayed detailed information about a client node

Display complete information about the client node named Joe.

```
query node joe format=detailed
```

```
                          Node Name: JOE
                           Platform: WinNT
                  Client OS Level: 4.00
                   Client Version: Version 5, Release 4,
                                   Level 0.0
              Application Version: Version 6, Release 4,
                                   Level 0.4
```

```
                  Policy Domain Name: STANDARD
               Last Access Date/Time: 09/24/2012 18:55:46
              Days Since Last Access: 6
              Password Set Date/Time: 09/24/2012 18:26:43
            Days Since Password Set: 6
              Invalid Sign-on Count: 0
                            Locked?: No
                            Contact:
                        Compression: Client
          Archive Delete Allowed?: Yes
           Backup Delete Allowed?: No
           Registration Date/Time: 09/24/2012 18:26:43
        Registering Administrator: SERVER_CONSOLE
Last Communication Method Used: Tcp/Ip
   Bytes Received Last Session: 108,731
       Bytes Sent Last Session: 698
    Duration of Last Session: 0.00
   Pct. Idle Wait Last Session: 0.00
  Pct. Comm. Wait Last Session: 0.00
  Pct. Media Wait Last Session: 0.00
                     Optionset:
                           URL: http://joe.host.name:1581
                     Node Type: Client
     Password Expiration Period: 60
              Keep Mount Point?: No
  Maximum Mount Points Allowed: 2
         Auto Filespace Rename: No
             Validate Protocol: No
                   TCP/IP Name:
                TCP/IP Address: 9.11.153.39
            Globally Unique ID: 11.9c.54.e0.8a.b5.11.d6.b3.
                                c3.00.06.29.45.cl
          Transaction Group Max: 0
                Data Write Path: ANY
                 Data Read Path: ANY
            Session Initiation: ClientOrServer
            High-level Address:
             Low-level Address: 1501
       Collocation Group Name:
             Proxynode Target:
              Proxynode Agent:
                  Node Groups:
                Email Address:
                Deduplication: ServerOnly
```

AIX | Linux

```
                Users allowed to back up: ALL
              Replication State: Enabled
               Replication Mode: Send
        Backup Replication Rule: DEFAULT
      Archive Replication Rule: ALL_DATA
Space Management Replication Rule: None
     Replication Primary Server: PRODSERVER1
      Last Replicated to Server: DRSERVER1
           Client OS Name: WIN: Windows XP
  Client Processor Architecture: x86
      Client Products Installed: WIN, FCM, VE
          Client Target Version:
             Version 6, Release 2, Level 0.0
                 Authentication: Local
                   SSL Required: No
              Session Security: Strict
              Transport Method: TLS 1.2
         Split Large Objects: Yes
                At-risk type: Default interval
           At-risk interval:
                Utility URL:
Replication Recovery of Damaged Files: Yes
                Decommissioned:
           Decommissioned Date:
```

Field descriptions

Node Name

The name of the client node.

Platform
: The operating system of the client node, as of the last time that the client node contacted the server. A question mark (?) is displayed until the client node first accesses the server and reports its operating system type.

Client OS Level
: The level of the operating system for the client as of the last time that the client node contacted the server.

Client Version
: The version of the client that is installed on the client node.

  This field does not apply to NAS nodes.

Application Version
: The version of the Data Protection for VMware client.

Policy Domain Name
: The assigned policy domain of the client node.

Last Access Date/Time
: The last date and time that the client node accessed the server.

Days Since Last Access
: The number of days that elapsed since the last time that the client node accessed the server.

Password Set Date/Time
: The date and time that the password was set for the client node.

Days Since Password Set
: The number of days that elapsed since the password was set for the client node.

Invalid Sign-on Count
: The number of invalid sign-on attempts that were made since the last successful sign-on. This count can be non-zero only when the invalid password limit (SET INVALIDPWLIMIT) is greater than zero. When the number of invalid attempts equals the limit that is set by the SET INVALIDPWLIMIT command, the node is locked out of the system.

Locked?
: Whether the client node is locked out of IBM Spectrum Protect.

Contact
: Any contact information for the client node.

Compression
: Whether compression is enabled on the client node.

  This field does not apply to NAS nodes.

Archive Delete Allowed?
: Whether the client node can delete its own archive files.

Backup Delete Allowed?
: Whether the client node can delete its own backup files.

Registration Date/Time
: The date and time that the client node was registered.

Registering Administrator
: The name of the administrator that registered the client node.

Last Communication Method Used
: The communication method that was last used by the client node to contact the server.

Bytes Received Last Session
: The number of bytes received by the server during the last client node session.

  This field does not apply to NAS nodes.

Bytes Sent Last Session
: The number of bytes sent to the client node.

  This field does not apply to NAS nodes.

Duration of Last Session
: How long the most recent client node session lasted, in seconds.

  This field does not apply to NAS nodes.

Pct. Idle Wait Last Session
: The percentage of the total session time that the client was not running any functions.

  This field does not apply to NAS nodes.

Pct. Comm. Wait Last Session
: The percentage of the total session time that the client waited for a communication response from the server.

  This field does not apply to NAS nodes.

Pct. Media Wait Last Session
: The percentage of the total session time that the client waited for a removable volume to be mounted.

  This field does not apply to NAS nodes.

Optionset
: The name of the client option set.

URL
: The URL of the IBM Spectrum Protect web client that is configured on the client system. You can use the URL in a web browser and in the Operations Center to remotely manage the client node.

Node Type
: The type of client node. One of the following values is possible:

  - Client: a backup-archive client, an IBM Spectrum Protect for Space Management client, or an application client
  - Server: an IBM Spectrum Protect server
  - NAS: a NAS file server

Password Expiration Period
: The password expiration period of the client node.

Keep Mount Point?
: Whether the client node retains a mount point during a session.

Maximum Mount Points Allowed
: The number of mount points that a client node can use on the server for IBM Spectrum Protect for Space Management migration and for backup and archive operations. This parameter does not apply to nodes with a type of NAS or SERVER. If a client node was registered to a server at Version 3.7 or later, the value is 0-999, depending on the value that is set with the MAXNUMMP parameter of the REGISTER NODE command. If the client node was registered under previous versions of the server and the MAXNUMMP parameter was not explicitly set by using the UPDATE NODE command, the value is set to NOLIMIT. The MAXNUMMP value is not evaluated or enforced during client data read operations such as restore, retrieve, and IBM Spectrum Protect for Space Management recall. However, mount points in use for data read operations are evaluated against attempted concurrent data store operations for the same client node. This evaluation might prevent the data store operations from acquiring mount points.

Auto Filespace Rename
: Whether IBM Spectrum Protect prompts the client to rename file spaces when the client system upgrades to a client that supports Unicode. This field is valid only for client systems that use Windows, Macintosh OS X, or NetWare operating systems.

Validate Protocol (deprecated)
: Whether the client has data validation enabled. If the client has data validation enabled, this field specifies whether IBM Spectrum Protect validates only the file data or all data, which includes file metadata. You can enable data validation by using the REGISTER NODE or UPDATE NODE command. This field is deprecated.

TCP/IP Name
: The host name of the client node as of the last time that the client node contacted the server. The field is blank if the client software does not support reporting this information to the server.

TCP/IP Address
: The TCP/IP address of the client node as of the last time that the client node contacted the server. The field is blank if the client software does not support reporting this information to the server.

Globally Unique ID
: The globally unique identifier (GUID) as of the last time that the client node contacted the server. This GUID identifies the host computer on which the node is located.

Transaction Group Max
: Specifies the number of files per transaction committed that are transferred between a client and a server. Client performance might be improved by using a larger value for this option.

Data Write Path
: Specifies the transfer path that is used when the client sends data to the server, storage agent, or both, during storage operations. If a path is unavailable, the node cannot send any data.

  AIX Linux Data transfer path options are ANY, LAN, or LAN-free.

Data Read Path
: Specifies the transfer path that is used when the server, storage agent, or both, read data for a client, during operations such as restore or retrieve. If a path is unavailable, data cannot be read.

  AIX Linux Data transfer path options are ANY, LAN, or LAN-free.

Session Initiation
: Controls whether the server or client initiates sessions. The following two options are available:

  - ClientOrServer
  - Serveronly

High-level Address
: Specifies the client IP address that the server contacts to initiate scheduled events when SESSIONINITIATION is set to SERVERONLY.

Low-level Address
: Specifies the client port number on which the client listens for sessions from the server when SESSIONINITIATION is set to SERVERONLY.

Collocation Group Name
: Specifies the name of the collocation group to which a node belongs. If a node does not belong to a collocation group, this field is blank.
  Tip: If the node contains file spaces that are members of a file space collocation group, this field is left blank. You can find file space names by issuing the QUERY FILESPACE command.

Proxynode Target
: Specifies which nodes are proxy nodes (agents) for other nodes, in a space-separated list. If there are no nodes in that type of association, this field is blank.

Proxynode Agent
: Specifies the originating (target) node name for a proxy node session, in a space separated list. If there are no nodes in that type of association, this field is blank.

Node Groups
: Specifies the name of the node group to which a node belongs. If a node does not belong to a node group, this field is blank.

Email Address
: Specifies the email address of the client node.

Deduplication
: The location where data is deduplicated. The value ServerOnly specifies that data stored by this node can be deduplicated on the server only. The Clientorserver value specifies that data stored by this node can be deduplicated on either the client or the server.

AIX Linux Users allowed to back up
: AIX Linux Specifies whether a non-root user ID or only a root user ID can back up files to the server. ALL indicates all users, while ROOT indicates that just the root user ID can back up files to the server. This output is not available if the client node operating system is considered a single-user operating system.

Replication State
: Indicates whether the node is enabled for replication. The following values are possible:

  Enabled
  : The node is configured for replication and ready to replicate.

  Disabled
  : The node is configured for replication but is not ready to replicate.

  None
  : The node is not configured for replication.

Replication Mode
: Indicates whether the node is configured as the source of or target for replicated data. If this field is blank, the node is not configured for replication. The following values are possible:

  Send
  : The node is configured as the source of data for replication.

  Receive
  : The node is configured as the target of data for replication.

  SyncSend
  : The data that belongs to the node is to be synchronized with the node data that is on the target replication server. Synchronization applies only to nodes whose data was imported from a source replication server and imported to the target replication server. Synchronization occurs during replication.

  SyncReceive

The data that belongs to the node is to be synchronized with the node data that is on the source replication server. Synchronization applies only to nodes whose data was imported from a source replication server and imported to the target replication server. Synchronization occurs during replication.

None
The node is not configured for replication.

Replication Primary Server
Specifies the source replication server for the client node.

Backup Replication Rule
Archive Replication Rule
Space Management Replication Rule
The replication rule that applies to back up, archive, and space-managed data that belongs to the node. The following values are possible:

ALL_DATA
Replicates backup, archive, or space-managed data. The data is replicated with normal priority.

ACTIVE_DATA
Replicates active backup data. The data is replicated with normal priority.
Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

- When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
- When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
- When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
Replicates backup, archive, or space-managed data. The data is replicated with high priority.

ACTIVE_DATA_HIGH_PRIORITY

This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

DEFAULT
Replicates backup, archive, or space-managed data according to the domain rule for the data type.

NONE
No data is replicated. For example, if the replication rule for archive data is NONE, archive data that belongs to the node is not replicated.

Last Replicated to Server
Specifies the name of the server that the node was last replicated to and the name of the server that the client fails over to during restore operations.

Client OS Name
The operating system of the client. The client deployment wizard uses this information to deploy a package to the client. This field is reported only for IBM Spectrum Protect clients at V6.2.0.0 and later.

Client Processor Architecture
The client architecture. The client deployment wizard uses this value to determine which package to deploy when the client is being updated. This field is reported only for IBM Spectrum Protect clients at V6.2.0.0 and later.

Client Products Installed
The products that are on the node. The following products might be listed:

- BA (Backup-Archive Client)
- VE (Virtual Environments)
- FCM (FlashCopy® Manager)

Client Target Version
The version of the client that is installed at a time that is scheduled through the DEFINE SCHEDULE or UPDATE SCHEDULE command. This field is reported only for IBM Spectrum Protect clients at V6.2.0.0 and later.

Authentication
Specifies the password authentication method: LOCAL, LDAP, or LDAP (pending).

Authentication Target	**Authentication Method**

Authentication Target	Authentication Method
IBM Spectrum Protect server	LOCAL
LDAP directory server	LDAP
This node is configured to authenticate with an LDAP directory server, but the node did not yet authenticate.	LDAP (pending)

SSL Required (deprecated)

Specifies whether the security setting for the node requires the Secure Sockets Layer (SSL) protocol. Values can be YES, NO, or Default. You must have system level authority to update the node SSLREQUIRED setting. This field is deprecated.

Session Security

Specifies the level of session security that is enforced for the node. Values can be STRICT or TRANSITIONAL.

Transport Method

Specifies the transport method that was last used for the specified node. Values can be TLS 1.2, TLS 1.1, or NONE. A question mark (?) is displayed until a successful authentication is completed.

Split Large Objects

Specifies whether large objects that are stored by this node are automatically split into smaller pieces, by the server, to optimize server processing. Yes indicates that the server splits large objects (over 10 GB) into smaller pieces when stored by a client node. No indicates that this process is bypassed. The default value is Yes.

At-risk type

Specifies the at-risk evaluation type. Values can be Default, Bypassed, or Custom. Default indicates that the node is evaluated with the same interval that was specified for the nodes classification by the SET STATUSATRISKINTERVAL command. Bypassed indicates that the node is not evaluated for at-risk status by the status monitor. Custom indicates that the node is evaluated with the interval that was specified by the SET NODEATRISKINTERVAL command, rather than the interval that was specified by the SET STATUSATRISKINTERVAL command.

At-risk interval

Specifies the number of hours between two client backup activities, or two replication activities, after which the status monitor indicates that the activity is at risk. This field contains a value only when the `At-risk type` field contains the value of `Custom`.

Utility URL

Specifies the address of the IBM Spectrum Protect client management services that are configured on the client system. This URL is used by the Operations Center to access client log files so that you can remotely diagnose client issues from the Operations Center.

Replication Recovery of Damaged Files

Specifies whether damaged files can be recovered for this node from a target replication server.

Decommissioned

Specifies whether the client node is decommissioned. The following values are possible:

YES
: Specifies that the node is decommissioned.

Null value
: Specifies that the node is not decommissioned.

PENDING
: Specifies that the node is being decommissioned, or the decommission process failed.

Tip: If you want to determine the status of a pending decommission process, follow the instructions in Decommissioning a client node.

Decommissioned Date

Specifies the date that the client node was decommissioned.

Example: Display information about node roles

The example output is only a portion of the full display.

```
query node alvin f=d

                 Proxynode Agent:
                     Node Groups:
                   Email Address:
                   Deduplication: ServerOnly
       Users allowed to back up: All
```

```
                  Role: Server
         Role Override: UseReported
      Processor Vendor: ORACLE
       Processor Brand: UltraSPARC-T2
        Processor Type: 4
       Processor Model:
       Processor Count: 1
            Hypervisor:
       API Application: NO
            Scan Error: NO
           MAC Address:
```

Field Descriptions

Role
: The processor role as reported by the client.

Role Override
: The override value for role, which is specified with the UPDATE NODE command.

Processor Vendor
: The processor vendor as reported by the client.

Processor Brand
: The processor brand as reported by the client.

Processor Type
: The processor type as reported by the client. This value specifies the number of processor cores that are used for PVU calculation.

Processor Model
: The processor model as reported by the client.

Processor Count
: The processor count as reported by the client.

Hypervisor
: The hypervisor as reported by the client.

API Application
: The client indicator that the client is an API application.

Scan Error
: The indicator of whether the latest scan for processor information might be failing and needs investigation.

MAC Address
: MAC Address as reported by the client.

Example: View all nodes that authenticate to the IBM Spectrum Protect server

If you want to view all nodes that authenticate locally, specify the following command:

```
query node * authentication=local
```

```
Node    Platform  Policy       Days Since   Days Since   Locked?
Name              Domain Name  Last Access  Password Set
_____________________________________________________________
NODE1   WinNT     STANDARD         3            3          No
LOCAL   (?)       STANDARD         7            7          No
```

Related commands

Table 1. Commands related to QUERY NODE

Command	Description
LOCK NODE	Prevents a client from accessing the server.
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
QUERY REPLNODE	Displays information about the replication status of a client node.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

Command	Description
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
REMOVE REPLNODE	Removes a node from replication.
RENAME NODE	Changes the name for a client node.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
RESET PASSEXP	Resets the password expiration for nodes or administrators.
SET INVALIDPWLIMIT	Sets the number of invalid logon attempts before a node is locked.
SET MINPWLENGTH	Sets the minimum length for client passwords.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
UNLOCK NODE	Enables a locked user in a specific policy domain to access the server.
UPDATE NODE	Changes the attributes that are associated with a client node.

QUERY NODEDATA (Query client data in volumes)

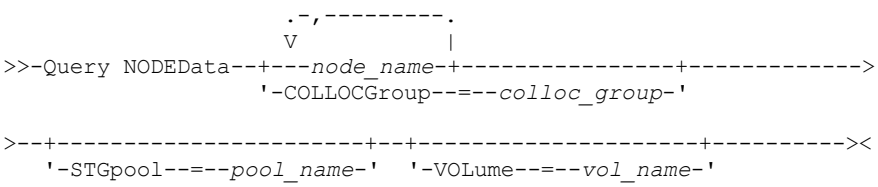
Use this command to display information about the data for one or more nodes in a sequential access storage pool. QUERY NODEDATA displays the name of the volume on which a node's data is written and the amount of space that is occupied by the data on that volume. This information is useful when you determine how to group nodes into collocated storage pools.

Privilege class

Restriction: You cannot use this command to display information for container storage pools.

Any administrator can issue this command.

Syntax



Parameters

node_name
: Specifies the name of the client node for which you want to locate data. You can specify one or more names. If you specify multiple names, separate the names with commas; do not use intervening spaces. You can also use wildcard characters to specify multiple names. You must specify either a node name or collocation group name, but not both.

COLLOCGroup
: Specifies the name of the collocation group for which you want to locate data. You must specify either a node name or collocation group name, but not both.
Important: If the amount of space that is needed to complete the query about a collocation group exceeds the SQL buffer limit, the QUERY NODEDATA command can fail. If the command fails for this reason, issue the QUERY COLLOCGROUP command to display a list of nodes in the group. Then, issue the QUERY NODEDATA command for each node in the group.

STGpool

Specifies the name of the sequential storage pool to query. This parameter is optional. You can use wildcard characters to specify the names. If a wildcard matches the name of a disk storage pool, the name of the disk storage pool is ignored. If you do not specify a value for this parameter, all sequential storage pools are queried.

VOLume

Specifies the volume that contains the data. This parameter is optional. You can use wildcard characters to specify multiple names. If you do not specify a value for this parameter, all volumes in the storage pool are queried.

Use wildcards to display node data for a sequential access storage pool

Display information about where node data is stored in a sequential storage pool. Use a wildcard character to indicate node names. See Field descriptions for field descriptions.

```
query nodedata e*
```

```
   Node Name   Volume Name                      Storage Pool  Physical
                                                Name          Space
                                                              Occupied
                                                              (MB)
   ---------   ------------------------------   ------------  --------
   EDU_J2      E:\tsm\server\00000117.BFS       EDU512        0.01
   EDU_J2      E:\tsm\server\00000122.BFS       EDU319        0.01
   EDU_J3      E:\tsm\server\00000116.BFS       EDU512        0.01
   EDU_J3      E:\tsm\server\00000120.BFS       EDU319        0.01
   EDU_J7      E:\tsm\server\00000118.BFS       EDU512        0.04
   EDU_J7      E:\tsm\server\00000123.BFS       EDU319        0.04
   EDU_JJ1     E:\tsm\server\00000116.BFS       EDU512        0.01
   EDU_JJ1     E:\tsm\server\00000121.BFS       EDU512        0.01
```

Display node data information for a specific collocation group

Display information about the location of node data in a sequential storage pool for a particular collocation group. In this example, nodes EDU_J3 and EDU_JJ1 are the only members that belong to collocation group, grp1, and have data in a sequential access storage pool.

```
query nodedata collocgroup=grp1
```

```
   Node Name   Volume Name                      Storage Pool  Physical
                                                Name          Space
                                                              Occupied
                                                              (MB)
   ---------   ------------------------------   ------------  --------
   EDU_J3      E:\tsm\server\00000116.BFS       EDU512        0.01
   EDU_J3      E:\tsm\server\00000120.BFS       EDU319        0.01
   EDU_JJ1     E:\tsm\server\00000116.BFS       EDU512        0.01
   EDU_JJ1     E:\tsm\server\00000121.BFS       EDU512        0.01
```

If you specify a file space collocation group, only the volumes of the file spaces that belong to the collocation group are displayed. If you specify a file space collocation group and a volume, the file space volumes within the collocation group that are also in the specified volume are displayed.

Field descriptions

Node Name

Specifies the name of the node.

Volume Name

Specifies the name of the volume that contains the node data.

Storage Pool Name

Specifies the name of the storage pool in which the volume is located.

Physical Space Occupied (MB)

Specifies the amount of physical space that is occupied by the node's data. Physical space includes empty space within aggregates, from which files might be deleted or expired.

Related commands

Table 1. Commands related to QUERY NODEDATA

Command	Description

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE COLLOCGROUP	Updates the description of a collocation group.
UPDATE STGPOOL	Changes the attributes of a storage pool.

QUERY NODEGROUP (Query a node group)

Use this command to display the node groups defined on the server.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*----------.
>>-Query NODEGroup--+------------+------------------------------>
                    '-group_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

group_name
: Specifies the name of the node group to display. To specify multiple names, use a wildcard character. This parameter is optional. The default is to display all node groups.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed. To display the members of the node group, you must specify FORMAT=DETAILED.

Example: List node groups on the server

Display the node groups defined on the server. See Field descriptions for field descriptions.

```
query nodegroup

Node Group Name              Node Group Description
-------------------------    ------------------------------
DEPT_ED                      Education department
GROUP1                       Low cap client nodes.
```

Example: Display detailed node group information

Display complete information about all node groups and determine which client nodes belong to which node groups. See Field descriptions for field descriptions.

```
query nodegroup format=detailed

               Node Group Name: DEPT_ED
        Node Group Description: Education department
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2006 10:59:03
          Node Group Member(s): EDU_1 EDU_7

               Node Group Name: GROUP1
        Node Group Description: Low cap client nodes.
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 04/21/2006 10:59:16
          Node Group Member(s): CHESTER REX NOAH JARED
```

Field descriptions

Node Group Name
: The name of the node group.

Node Group Description
: The description for the node group.

Last Update by (administrator)
: The name of the administrator that defined or most recently updated the node group.

Last Update Date/Time
: The date and time that an administrator defined or most recently updated the node group.

Node Group Member(s)
: The members of the node group.

Related commands

Table 1. Commands related to QUERY NODEGROUP

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.
UPDATE NODEGROUP	Updates the description of a node group.

QUERY OCCUPANCY (Query client file spaces in storage pools)

Use this command to show where client file spaces are stored and how much space they occupy.

Privilege class

Any administrator can issue this command.

Syntax

Parameters

node_name
: Specifies the node that owns the file spaces that you want to locate. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all nodes are queried.

file_space_name
: Specifies the file space that you want to locate. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all file spaces are queried. You must specify a node name if you specify a file space name.

  For a server that has clients with Unicode support, you might need to have the server convert the file space name that you enter. For example, you might need to have the server convert the name that you enter from the server's code page to Unicode. See the NAMETYPE parameter for details. If you do not specify a file space name or specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or non-Unicode file spaces.

STGpool
: Specifies the storage pool to query for files from the specified file space. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all storage pools are queried.

DEVclass
: Specifies the device class that is associated with the devices where the file spaces are stored. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, storage pools that are associated with any device class are queried.

Type
: Specifies the types of files to query in the file spaces. This parameter is optional. The default value is ANY. Possible values are:

  ANY
  : Specifies that all types of files are queried: back up versions of files, archived copies of files, and files that are migrated from IBM Spectrum Protect™ for Space Management clients.

  Backup
  : Specifies that backup files are queried.

  Archive

Specifies that archive files are queried.

SPacem
: Specifies that space-managed files (files that were migrated by an IBM Spectrum Protect for Space Management client) are queried.

NAMEType
: Specifies how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with Unicode support. A backup-archive client with Unicode support is available only for Windows, Macintosh OS 9, Macintosh OS X, and NetWare. Use this parameter only when you specify a partly or fully qualified file space name.

  The default value is SERVER. Possible values are:

  SERVER
  : The server uses the server's code page to interpret the file space names.

  UNIcode
  : The server converts the file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the names and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has a problem accessing system conversion routines.

  FSID
  : The server interprets the file space names as their file space IDs (FSIDs).

CODEType
: Specifies how you want the server to interpret the file space names that you enter. Use this parameter only when you enter a single wildcard character for the file space name or when you do not specify any file space name.

  The default value is BOTH, which means that the file spaces are included regardless of code page type. Possible values are:

  UNIcode
  : Include file spaces that are only Unicode enabled.

  NONUNIcode
  : Include file spaces that are not only Unicode enabled.

  BOTH
  : Include file spaces regardless of code page type.

Example: Display file spaces assigned to a specific node

Display information about where all file spaces assigned to the node named DAISY are stored. See Field descriptions for field descriptions.

```
query occupancy daisy
```

```
Node     Type  Filespace    FSID  Storage    Number    Physical    Logical
Name           Name               Pool       of        Space       Space
                                  Name       Files     Occupied    Occupied
                                                       (MB)        (MB)
-------  ----  ----------  -----  ---------  --------  -------     --------
 DAISY   Bkup  DRIVED        1    COPYFILE      38      0.45         0.42
```

Example: Display file spaces assigned to a specific node with a backup file type

Display information about the file spaces that belong to the node WAYNE, and that have a backup file type. See Field descriptions for field descriptions.

```
query occupancy wayne type=backup
```

```
 Node    Type  Filespace FSID   Storage      Number  Physical    Logical
 Name          Name              Pool         of      Space       Space
                                 Name         Files   Occupied    Occupied
                                                      (MB)        (MB)
 ------  -----  ---------  -----  -----------  -------  ---------  --------
 WAYNE   Bkup   DWG1         1    BACKUPPOOL1  2,330    53.19      50.01
 WAYNE   Bkup   OS2C         2    BACKUPPOOL1  1,554    32.00      31.30
```

Field descriptions

Node Name
The node that owns the file space. If the node was previously deleted, the node name DELETED is displayed.

Type
The type of data. Possible values are:

Arch
Data that has been archived.

Bkup
Data that has been backed up.

SpMg
Data that has been migrated from an IBM Spectrum Protect for Space Management client.

Filespace Name

The name of the file space that belongs to the node.

If the file space was previously deleted, the file space name DELETED is displayed.

File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

Storage Pool Name
The storage pool where the file space is located.

Number of Files
The number of logical files that belong to the file space and are stored in this storage pool. When storing a file larger than 10 GB, the server splits the file into 10 GB fragments. The number of fragments is also included in this value for occupancy calculations.

Physical Space Occupied (MB)
The amount of physical space that is occupied by the file space. Physical space includes empty space within aggregates, from which files might have been deleted or expired. For this value, 1 MB = 1048576 bytes.
Tip: This field does not display a value for storage pools that are set up for data deduplication. If you turn off data deduplication for a storage pool, a value for physical occupancy is not displayed until the storage pool is empty of deduplicated files.

Logical Space Occupied (MB)
The amount of space that is occupied by logical files in the file space. Logical space is the space that is actually used to store files, excluding empty space within aggregates. For this value, 1 MB = 1048576 bytes.

FSID
The file space ID (FSID) for the file space. The server assigns a unique FSID when a file space is first stored on the server.

Related commands

Table 1. Commands related to QUERY OCCUPANCY

Command	Description
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.

QUERY OPTION (Query server options)

Use this command to display information about server options.

Change server options by editing the server options file or by issuing the SETOPT command. When you edit the server options file, you must restart the server before any changes take effect. Any changes you make by issuing the SETOPT command take effect immediately.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-*----------.
>>-Query OPTion--+------------+--------------------------------><
                '-optionname-'
```

Parameters

optionname
: Specifies the name of an option in the server options file. This parameter is optional. You can use wildcard characters to specify this name. All matching server options display. If you do not specify this parameter, information on all options displays.

Example: Display all server options

Display general information about all server options. The output lists all options with their specified values.

```
query option
```

Example: Display options settings using a wildcard character

View the option settings for all options that begin with L.

```
query option l*

Server Option         Option Setting
-----------------     --------------------
Language              AMENG
```

Example: Display LDAP directory servers

View the settings for all LDAP directory servers.

```
query option ldapurl

Server Option         Option Setting
-----------------     --------------------
LDAP URL               ldap:\\tophoy.tucson.com\cn=tsmdata
LDAP URL               ldap:\\krypton.ibm.com\ou=tsmdata,dc=ibm,dc=com
```

Field descriptions

Server Option
: Specifies the name of the option in the server options file.

Option Setting
: Specifies the name of the option in the server options file.

Related commands

Table 1. Commands related to QUERY OPTION

Command	Description
SETOPT	Updates a server option without stopping and restarting the server.

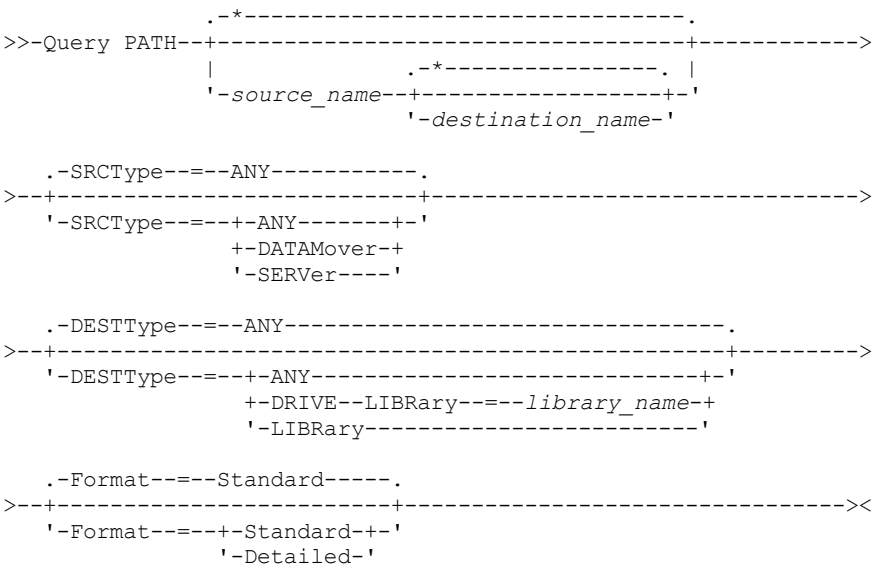
QUERY PATH (Display a path definition)

Use this command to display the path between a source and a destination.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

source_name
: Specifies the name of a source for which to display paths. This parameter is optional. You can specify wildcard characters. The default is to display paths for all sources.

  A source is a data mover, a server, or a storage agent.

destination_name
: Specifies the name of a destination for which to display paths. This parameter is optional. You can specify wildcard characters. The default is to display paths for all destinations.

SRCType
: Specifies the type of the source. This parameter is optional. The default is to display paths for all source types. Possible values are:

  ANY
  : Specifies to display paths with any source type.

  DATAMover
  : Specifies to only display paths with the DATAMOVER source type.

  SERVer
  : Specifies to only display paths with the SERVER source type. (A source that has a source type of SERVER is a storage agent.)

DESTType
: Specifies the type of the destination. This parameter is optional. The default is to display paths for all destination types. Possible values are:

  ANY
  : Specifies to display paths with any destination type.

  DRive

Specifies to display only paths with the DRIVE destination type. When the destination type is a drive, you must specify the library name. You can refine which paths are displayed by entering a name in the LIBRARY parameter.

LIBRary
Specifies that only paths with destination type LIBRARY display.

LIBRary
Specifies the name of the library to which the drive belongs. This parameter is required when the destination type is a drive (DESTTYPE=DRIVE).

Format
Specifies how the information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

Standard
Specifies that partial information is displayed.

Detailed
Specifies that complete information is displayed.

Example: Display summary path information

Display information about paths for the source NETAPP1. See Field descriptions for field descriptions.

```
query path netapp1
```

```
Source Name  Source Type  Destination Name  Destination Type  Online
-----------  -----------  ----------------  ----------------  ------
NETAPP1      DATAMOVER    DRIVE1            DRIVE             Yes
NETAPP1      DATAMOVER    NASLIB            LIBRARY           Yes
```

Example: Display detailed path information

Display detailed information about paths for the source NETAPP1. See Field descriptions for field descriptions.

```
query path netapp1 format=detailed
```

Linux

```
                 Source Name: NETAPP1
                 Source Type: DATAMOVER
            Destination Name: NASLIB
            Destination Type: LIBRARY
                     Library:
                      Device: /dev/tsmscsi/mc0
                   Directory:
                     On-Line: Yes
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 06/21/2002 20:52:56

                 Source Name: NETAPP1
                 Source Type: DATAMOVER
            Destination Name: DRIVE1
            Destination Type: DRIVE
                     Library: NASLIB
                      Device: rst0l
                   Directory:
                     On-Line: Yes
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 06/21/2002 20:55:23
```

AIX | Windows

```
                 Source Name: NETAPP1
                 Source Type: DATAMOVER
            Destination Name: NASLIB
            Destination Type: LIBRARY
                     Library:
                      Device: mc0
                   Directory:
                     On-Line: Yes
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 06/21/2001 20:52:56

                 Source Name: NETAPP1
```

```
                Source Type: DATAMOVER
           Destination Name: DRIVE1
           Destination Type: DRIVE
                    Library: NASLIB
                     Device: rst01
                  Directory:
                    On-Line: Yes
Last Update by (administrator): SERVER_CONSOLE
     Last Update Date/Time: 06/21/2001 20:55:23
```

AIX Linux

Example: Display detailed path information for a z/OS media server

Display detailed information about a z/OS® media server path. See Field descriptions for field descriptions.

```
query path format=detailed
```

```
                Source Name: SERVER1
                Source Type: SERVER
           Destination Name: ZOSMEDIA
           Destination Type: LIBRARY
                    Library:
                  Node Name:
                     Device:
           External Manager:
           ZOS Media Server: MEDSERV1
                Comm. Method:
                        LUN:
                  Initiator: 0
                  Directory:
                    On-Line: Yes
Last Update by (administrator): ADMIN
     Last Update Date/Time: 06/08/2011 15:33:39
```

Field descriptions

Source Name
: The name of the source.

Destination Name
: The name of the destination.

Source Type
: The type of the source.

Destination Type
: The type of the destination.

Library
: The name of the library that contains the drive that is the destination.

  This field will be blank if the destination type is library. The library name is in destination name field when the destination is a library.

Node Name
: The name of the device that is the destination.

Device
: The name of the device that is the destination.

External Manager
: The name of the external manager.

ZOS Media Server
: The name of the z/OS media server.

Comm. Method
: Specifies the type of communication method.

LUN
: Specifies the logical unit name through which the disk can be accessed by the source.

Initiator
: Specifies the initiator of the communication.

Directory
: Specifies the directory location of a file on the source.

On-Line
: Whether the path is online and available for use.

Last Update by (administrator)
: The ID of the administrator who performed the last update.

Last Update Date/Time
: The date and time when the last update occurred.

Related commands

Table 1. Commands related to QUERY PATH

Command	Description
DEFINE PATH	Defines a path from a source to a destination.
DELETE PATH	Deletes a path from a source to a destination.
UPDATE PATH	Changes the attributes associated with a path.

QUERY POLICYSET (Query a policy set)

Use this command to display information about one or more policy sets.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*--*------------------------------.
>>-Query POlicyset--+-----------------------------------+-------->
                    |              .-*---------------. |
                    '-domain_name--+-----------------+-'
                                   '-policy_set_name-'

   .-Format--=--Standard-----.
>--+-------------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

domain_name
: Specifies the policy domain associated with the policy set to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a value for this parameter, all policy domains are queried. You must specify this parameter when querying an explicitly named policy set.

policy_set_name
: Specifies the policy set to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify either ACTIVE or a policy set name, all policy sets are queried.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: List policy sets for all policy domains

Query all policy sets for all policy domains. Create the output in standard format. See Field descriptions for field descriptions.

```
query policyset
```

```
Policy        Policy        Default       Description
Domain        Set Name      Mgmt
Name                        Class
                            Name
---------     ---------     ---------     ------------------------
EMPLOYEE-     ACTIVE        ACTIVEFI-     Personnel Department
 _RECORDS                    LES
EMPLOYEE-     HOLIDAY       ACTIVEFI-     Personnel Department
 _RECORDS                    LES
EMPLOYEE-     VACATION      ACTIVEFI-     Personnel Department
 _RECORDS                    LES
PROG1         SUMMER                      Programming Group
                                           Policies
PROG2         SUMMER                      Programming Group
                                           Policies
STANDARD      ACTIVE        STANDARD      Installed default policy
                                           set.
STANDARD      STANDARD      STANDARD      Installed default policy
                                           set.
```

Example: Displayed detailed information about a specific policy set

Query the VACATION policy set that is in the EMPLOYEE_RECORDS policy domain. Create the output in detailed format. See Field descriptions for field descriptions.

```
query policyset employee_records vacation
format=detailed

            Policy Domain Name: EMPLOYEE_RECORDS
               Policy Set Name: VACATION
       Default Mgmt Class Name: ACTIVEFILES
                   Description: Personnel Department
Last Update by (administrator): $$CONFIG_MANAGER$$
         Last Update Date/Time: 05/31/1998 13:15:50
              Managing profile: ADSM_INFO
               Changes Pending: Yes
```

Field descriptions

Policy Domain Name
: The name of the policy domain.

Policy Set Name
: The name of the policy set.

Default Mgmt Class Name
: The management class assigned as the default for the policy set.

Description
: The description of the policy set.

Last Update by (administrator)
: The name of the administrator or server that most recently updated the policy set. If this field contains $$CONFIG_MANAGER$$, the policy set is associated with a domain that is managed by the configuration manager.

Last Update Date/Time
: The date and time when the policy set was most recently defined or updated.

Managing Profile
: The profile or profiles that manage the domain to which this policy set belongs.

Changes Pending
: Whether or not changes are being made but not activated. Once the changes are activated, the field resets to No.

Related commands

Table 1. Commands related to QUERY POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY POLICYSET	Creates a copy of a policy set.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.

Command	Description
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY DOMAIN	Displays information about policy domains.
UPDATE POLICYSET	Changes the description of a policy set.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

QUERY PROCESS (Query one or more server processes)

Use this command to display information about active background processes.

To cancel background processes, issue the CANCEL PROCESS command. To display detailed information about node replication processes, issue the QUERY REPLICATION command.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query PRocess--+----------------+---------------------------->
                  '-process_number-'

>--+------------------------+--+-------------------+----------><
   '-DESCription--=--string-'  '-STATus--=--string-'
```

Parameters

process_number
: Specifies the number of the background process to be queried. This parameter is optional. If not specified, information about all background processes is displayed.

DESCription
: Specifies a text string that you want to search for in the list of active processes' descriptions. Enclose the string expression in quotation marks if it contains blanks. You can use text and a wildcard character to specify this string. This parameter is optional.

STATus
: Specifies a text string that you want to search for in the list of active processes' statuses. Enclose the string expression in quotation marks if it contains blanks. You can use text and a wildcard character to specify this string. This parameter is optional.

Example: Query a single background process

Display information about background process 202. See Field descriptions for field descriptions.

```
query process 202
```

```
Process   Process             Process
Number    Description         Status
--------  -------------       ---------
     202  EXPORT SERVER       ANR0NNNI EXPORT
                              Identifier MYEXPORTSERVER
                              ANR0648I Have copied the
                              following: 8 Domains 2
                              Policy Sets 10 Management
                              Classes 4 Copy Groups 1
                              Administrators 746 Bytes
                              (0 errors have been
                              detected) Current input
                              volume(s): C:\BUILD\540\
```

```
                                GA\BUILD\NT\I386\DEBUG\
                                -00000014.BFS,(6 Seconds)
```

Example: Query all background processes

Display information about all background processes. See Field descriptions for field descriptions.

```
query process
```

```
Process   Process              Process
Number    Description          Status
--------  --------------       ---------
     304  IDENTIFY DUPLICATES  Storage Pool
                               FILEPOOL, Volume
                               /tsmpool2/00006664.
                               BFS, Files Processed:
                               2000, Duplicate Extents
                               Found: 344, Duplicate
                               Bytes Found: 3,238,123,
                               Current Physical File
                               (bytes): 2,626,676,296.
                               Status: Processing

     284  IDENTIFY DUPLICATES  Storage Pool
                               FILEPOOL, Volume
                               /tsmpool2/00006666.
                               BFS, Files Processed:
                               2000, Duplicate Extents
                               Found: 344, Duplicate
                               Bytes Found: 3,238,123,
                               Current Physical File
                               (bytes): None.
                               Status: Idle

       4  Replicate Node       Replicating Node(s) IRONMAN.
                               File spaces complete: 0. File
                               spaces identifying and
                               replicating: 1. File spaces
                               replicating: 0. File spaces
                               not started: 3. Files current:
                               11,920. Files replicated: 0
                               of 0. Files updated: 0 of 0.
                               Files deleted: 0 of 0. Amount
                               Replicated: 11,482 KB of 11,482
                               KB. Amount transferred: 11,482 KB.
                               Elapsed time: 0 Day(s), 0 Hour(s),
                               1 Minute(s).

      37  Expiration           Processed 12 nodes out of 30 total
                               nodes, examined 411 objects,
                               deleting 411 backup objects,
                               0 archive objects,
                               0 DB backup volumes,
                               0 recovery plan files;
                               0 objects have been retried and
                               0 errors encountered.
```

Example: Query all background replication processes

Display information about all background replication processes. See Field descriptions for field descriptions.

```
query process desc="replicate node"
```

```
Process   Process              Process
Number    Description          Status
--------  --------------       ---------
       4  Replicate Node       Replicating Node(s) IRONMAN.
                               File spaces complete: 0. File
                               spaces identifying and
                               replicating: 1. File spaces
                               replicating: 0. File spaces
                               not started: 3. Files current:
                               11,920. Files replicated: 0
```

```
                                of 0. Files updated: 0 of 0.
                                Files deleted: 0 of 0. Amount
                                Replicated: 11,482 KB of 11,482
                                KB. Amount transferred: 11,482 KB.
                                Elapsed time: 0 Day(s), 0 Hour(s),
                                1 Minute(s).
```

Example: Query all background replication processes for a specific node

Display information about all background replication processes. See Field descriptions for field descriptions.

```
query process desc="replicate node" status=ironman

Process   Process              Process
Number    Description          Status
--------  -------------        ---------
       4  Replicate Node       Replicating Node(s) IRONMAN.
                               File spaces complete: 0. File
                               spaces identifying and
                               replicating: 1. File spaces
                               replicating: 0. File spaces
                               not started: 3. Files current:
                               11,920. Files replicated: 0
                               of 0. Files updated: 0 of 0.
                               Files deleted: 0 of 0. Amount
                               Replicated: 11,482 KB of 11,482
                               KB. Amount transferred: 11,482 KB.
                               Elapsed time: 0 Day(s), 0 Hour(s),
                               1 Minute(s).
```

Example: Verify that a replication recovery process was initiated

After you start a node replication process with file recovery enabled, verify that the target replication server initiated the file recovery process. Issue the QUERY PROCESS command on the target replication server. For descriptions of fields, see Field descriptions.

```
query process

Process   Process Description   Process Status
Number
--------  -------------------   -------------------------------------
4         Replicate Node -      Replicating node(s) 3MAUTOIMPORT.
          Recovery.             File spaces complete: 87.
                                File spaces identifying and
                                replicating: 0.
                                File spaces replicating: 6.
                                File spaces not started: 0.
                                Files current: 0.
                                Files replicated: 0 of 14.
                                Files updated: 0 of 0.
                                Files deleted: 0 of 0.
                                Amount replicated:
                                0 KB of 11,688 bytes.
                                Amount transferred: 0 KB.
                                Elapsed time:
                                0 Day(s), 0 Hour(s), 1 Minute(s).
```

Example: Verify that damaged files are being recovered during a replication process

After you start a node replication process with file recovery enabled, verify that damaged files are being recovered. Issue the QUERY PROCESS command on the source replication server. For descriptions of fields, see Field descriptions.

```
query process

Process   Process Description   Process Status
Number
-------   -------------------   ------------------------
6         Replicate Node        Recovering damaged files
          (As Secondary         from server SERVER2,
           Recovery)            process 4, number of
                                active sessions 10.
```

AIX | Linux | Windows

Example: Verify that the files are being converted

After you start a storage pool conversion process, verify that the files are being converted. For descriptions of fields, see Field descriptions.

```
query process

Process  Process           Process
Number   Description       Status
-------  ---------------   -----------------------------------
6        Convert Stgpool   Converting storage pool FILEPOOL1
                           to directory-container storage pool
                           NEWDEDUP1. Volumes Converted: 1 of 6,
                           Volumes Failed: 0,
                           Converted Files: 975, Converted
                           Bytes: 196.27 MB, Skipped Files: 0,
                           Skipped Bytes: 0 B, Total Bytes
                           Transferred: 151.27 MB

7        Convert Stgpool   Converting storage pool DEDUPPOOL to
                           directory-container storage pool
                           DIRPOOL. Converted Files:  150 of 360,
                           Converted Bytes: 79,598 KB of 388 MB.
                           Unconverted Files: 12. Unconverted
                           Bytes: 27 MB. Current input volume:
                           /fvt/srv/BK01. Elapsed time: 0 Day(s),
                           0 Hour(s), 1 Minute(s).

8         Convert Stgpool  Converting storage pool FILEPOOL1 to
                           directory-container storage pool
                           NEWDEDUP1. Converted Files: 0,
                           Converted Bytes: 0 B of 1.00 GB,
                           Skipped Files: 0, Skipped Bytes: 0 B,
                           Total Bytes Transferred: 0 B,
                           Current input volume:
                           /STORAGE/file1/00000005.BFS,
                           Elapsed time: 0 Days, 0 Hours,
                           1 Minutes.

10        Convert Stgpool  Converting storage pool FILEPOOL1 to
                           directory-container storage pool
                           NEWDEDUP1. Converted Files: 1007,
                           Converted Bytes: 285.44 MB of 1.33 GB,
                           Skipped Files: 0, Skipped Bytes: 0 B,
                           Total Bytes Transferred: 196.28 MB,
                           Current input volume:
                           /STORAGE/file1/00000004.BFS,
                           Elapsed time: 0 Days, 0 Hours, 1 Minutes.
```

AIX | Linux | Windows

Example: Verify movement from local disk to the cloud

After the data-transfer operation from the local disk to the cloud starts, verify that the data is moving. For descriptions of fields, see Field descriptions.

```
query process


Process   Process          Process
Number    Description      Status
-------   --------------   ---------------------------------------
4         Local to Cloud   Local disk to cloud transfer for
          Transfer         directory-container storage pool
                           CLOUDPOOL. 1 container(s) processed.
                           2,100 KB in 4 data extent(s) transferred.
                           Elapsed time: 0 Day(s), 0 Hour(s),
                           1 Minute(s).
```

Field descriptions

Process Number
: Specifies the number that is assigned to the active background process.

Process Description
: Specifies a description of the active background process.

Process Status
: Specifies the status of the active background process.

Tip: When a node replication process is finished on the target replication server, only end process information is stored in the activity summary table. The full summary for the replication process is stored in the activity summary table on the source replication server.

Related commands

Table 1. Command related to QUERY PROCESS

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.
CANCEL PROCESS	Cancels a background server process.
IDENTIFY DUPLICATES	Identifies duplicate data in a storage pool.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLNODE	Displays information about the replication status of a client node.
RESTART EXPORT	Restarts a suspended export operation.
SUSPEND EXPORT	Suspends a running export operation.

QUERY PROFILE (Query a profile)

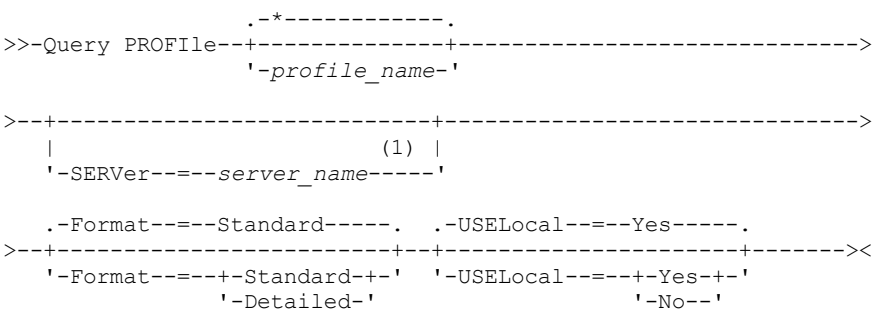
Use this command to display information about profiles and associated objects. Issue this command from a configuration manager or from a managed server. You can use this command to get profile information from any configuration manager defined to the server, even if the server does not subscribe to any profile.

If you query a locked profile from the configuration manager to which the profile belongs, complete profile information is displayed. If you query a locked profile from another server, the query displays only that the profile is locked.

Privilege class

Any administrator can issue this command.

Syntax



Notes:

1. The server name you specify depends on the server from which you issue the command. See the description of the SERVER parameter.

Parameters

profile_name
: Specifies the profile to display. To specify multiple names, use a wildcard character. This parameter is optional. The default is to display all profiles.

SERVer
: Specifies the configuration manager whose profile information is displayed. The requirements for the name depends on where the query is issued:

  - From a configuration manager: This parameter is optional. The default is the configuration manager's name.
  - From a managed server: This parameter is optional. The default is the name of the configuration manager for this managed server.
  - From a server that is neither a configuration manager nor a managed server: You must specify a name.

Format
: Specifies whether partial or detailed information is displayed. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that detailed information is displayed.

USELocal
: When you perform the query from a managed server, this parameter specifies whether the profile information is obtained from the configuration manager or the managed server. If the profile information does not exist on the managed server, the information is obtained from the configuration manager, regardless of the value of this parameter.

  If you use this parameter on a server that is not managed by the configuration manager that owns the profile, the parameter is ignored. The default value is YES. Possible values are:

  Yes
  : Specifies that the profile information, if available, is obtained from the managed server. The configuration manager is contacted if information is not available from the managed server.

  No
  : Specifies that the profile information is obtained from the configuration manager even if the information is available from the managed server. This ensures that you receive current information about the profile.

Example: List profiles from a configuration manager

Display profile information from a configuration manager. See Field descriptions for field descriptions.

```
query profile

Configuration       Profile name          Locked?
manager
---------------     ---------------       ------
SERVER1             DEFAULT_PROFILE       No
SERVER1             ADMIN_INFO            No
SERVER1             EMPLOYEE              No
SERVER1             PERSONNEL             Yes
```

Example: Display detailed profile information for a managed server

From a managed server, display current detailed information for profile ADMIN_INFO. See Field descriptions for field descriptions. Note: When the profile is locked, most fields are not displayed.

```
query profile admin_info
format=detailed uselocal=no

           Configuration manager: SERVER1
                    Profile name: ADMIN_INFO
                          Locked: No
                     Description: Distributed administrative schedules
```

```
            Server administrators: DENNIS EMILY ANDREA
                  Policy domains: ADMIN RECORDS
Administrative command schedules: ** all objects **
          Server Command Scripts:
              Client Option Sets:
                         Servers:
                   Server Groups:
```

Field descriptions

Configuration manager
: The name of the configuration manager that owns the profile.

Profile name
: The name of the profile.

Locked?
: Whether the profile is locked.

Description
: The description of the profile.

Server administrators
: The administrators that are associated with the profile.

Policy domains
: The policy domains that are associated with the profile.

Administrative command schedules
: The administrative schedules that are associated with the profile.

Server Command Scripts
: The server command scripts that are associated with the profile.

Client Option Sets
: The client option sets that are associated with the profile.

Servers
: The servers that are associated with the profile.

Server Groups
: The names of server groups that are associated with the profile.

Related commands

Table 1. Commands related to QUERY PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.
UPDATE PROFILE	Changes the description of a profile.

QUERY PROTECTSTATUS (Query the status of storage pool protection)

Use this command to display information about the status of storage pool protection for directory-container storage pools.

Privilege class

Any administrator can issue this command.

Syntax

```
                          .-*---------.
>>-Query PROTECTStatus--+-----------+--------------------------->
                          '-pool_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

pool_name
: Specifies the name of the directory-container storage pool to be queried. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value, the status of all directory-container storage pools is displayed.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Specify one of the following values:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display summary information about a specific storage pool

Display information about the storage pool that is named POOL1. Issue the following command:

```
query protectstatus pool1
```

```
Source         Source         Target         Target          Pct.        Last Complete
Server Name    Storage Pool   Server Name    Storage Pool    Protected   Protect
------------   ------------   ------------   ------------    ----------  --------------
NEXT           POOL1          NEXT           POOL1COPY       96.55       02/17/2017 11:15:07
NEXT           POOL1          NEXT1          POOL2           99.99       02/17/2017 11:14:53
NEXT           POOL1          UNKNOWN        UNKNOWN         UNKNOWN     02/17/2017 11:13:44
NEXT1          POOL2          NEXT           POOL1           100.00      02/17/2017 12:56:58
```

See Field descriptions for field descriptions.

Example: Display detailed information about a specific storage pool

Display information in full detail about the storage pool named, POOL1. Issue the following command:

```
query protectstatus pool1 format=detailed
```

```
       Source Server Name: NEXT
      Source Storage Pool: POOL1
       Target Server Name: NEXT
      Target Storage Pool: POOL1COPY
           Pct. Protected: 96.55
   Data Extents Protected: 1,747
       Data Extents Total: 1,852
           Protected (MB): 165.33
               Total (MB): 171.23
Last Completed Protection: 02/17/2017 11:15:07
   Last Refresh Date/Time: 02/19/2017 00:27:12
```

See Field descriptions for field descriptions.

Field descriptions

Source Server Name
: The name of the source server.

Source Storage Pool
: The name of the directory-container storage pool on the source server.

Target Server Name
: The name of the target server.

Target Storage Pool
: The name of the directory-container storage pool on the target server.

Pct. Protected
: The percentage of protected data in the directory-container storage pool.

Data Extents Protected
: The number of data extents that are protected in the directory-container storage pool.

Data Extents Total
: The total number of data extents in the directory-container storage pool.

Protected (MB)
: The total amount of protected data that is in the directory-container storage pool, in megabytes.

Total (MB)
: The total amount of data that is in the directory-container storage pool, in megabytes.

Last Completed Protection
: The date and time that the directory-container storage pool was last protected.

Last Refresh Date/Time
: The date and time that the directory-container storage pool was last refreshed.

Related commands

Table 1. Commands related to QUERY PROTECTSTATUS

Command	Description
PROTECT STGPOOL	Protects a directory-container storage pool.

QUERY PROXYNODE (Query proxy authority for a client node)

Use this command to display client nodes with authority to act as proxy to other client nodes in the IBM Spectrum Protect™ server.

Privilege class

Any administrator can issue this command.

Syntax

```
                                .-*----------------.
>>-Query PROXynode----TArget--=--+------------------+---------><
                                '-target_node_name-'
```

Parameters

TArget
: Specifies the name of the node targeted by the node with proxy authority. It is optional to specify a target node name. Wildcard names can be used to specify the target node name. A comma-separated list of node names is also allowed.

Example: List client nodes with proxy authority

To display all IBM Spectrum Protect client nodes with proxy authority to the target node named MYCLUSTER, issue the following command.

```
query proxynode target=mycluster

Target Node          Agent Node
---------------      ----------------
FRED                 MOE MINIE MICKEY
ALPHA                BETA GAMMA DELTA
```

Field descriptions

Target Node
: Specifies the name of the node targeted by the node with proxy authority.

Agent Node
: Specifies the name of the agent node.

Related commands

Table 1. Commands related to QUERY PROXYNODE

Command	Description
GRANT PROXYNODE	Grant proxy authority to an agent node.
REVOKE PROXYNODE	Revoke proxy authority from an agent node.

QUERY PVUESTIMATE (Display processor value unit estimate)

Use this command to obtain an estimate of the client devices and server devices that are being managed by the IBM Spectrum Protect™ server. In addition, this command provides an estimate of the processor value unit (PVU) totals for the server devices.

This command generates a PVU estimate that is based on the number of logical nodes that are defined to the IBM Spectrum Protect server. By contrast, the calculation of license obligations is based on the number of physical computers. There might not be a one-to-one correlation between the number of logical nodes and the number of physical computers. The report that is generated by the QUERY PVUESTIMATE command is an estimate, which is not legally binding.

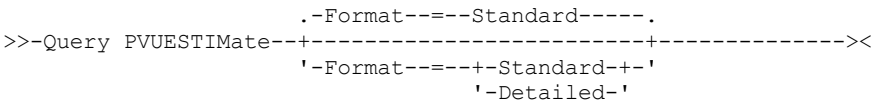
For purposes of the QUERY PVUESTIMATE command, nodes on Microsoft Windows 7, Microsoft Windows XP Professional, and Apple systems are assumed to be client devices. Nodes on all other platforms are considered to be server devices. The server on which IBM Spectrum Protect is running is also classified as a server device. However, you can reclassify server devices as client devices if required. If your system includes retired workstations, test workstations, or others that can be ignored for purposes of PVU calculation, you can specify them as type other. To change a node classification, use the UPDATE NODE command or the REGISTER NODE command.

Note: The PVU information reported by IBM Spectrum Protect is not considered an acceptable substitute for the IBM® License Metric Tool.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

Format
: Specifies the output format. This parameter is optional. The default is Standard. The following values can be used:

  Standard
  : Specifies standard output.

  Detailed
  : Specifies detailed output.

Example: Display the estimated number of devices and PVU

Display the estimated number of client devices and server devices, and the estimated PVU for the server devices, for an IBM Spectrum Protect server. Issue the following command:

```
query pvuestimate
```

Table 1. Sample output for several products managed by one IBM Spectrum Protect server

Product	Number of Client Devices	Number of Server Devices	PVU of Server Devices
IBM Spectrum Protect Extended Edition	1,000	905	90,500
IBM Spectrum Protect for Storage Area Networks	50	10	1,000
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect for Mail	0	25	5,000
IBM Spectrum Protect for Databases	0	1,025	20,500
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5,000
IBM Spectrum Protect for System Backup and Recovery	0	0	0

Other Node Classifications	Number
Nodes earlier than Version 6.3 with no PVU information available at this time	10
Nodes at Version 6.3 or later with no PVU match	9
Nodes classified by the administrator as "other-device"	8
Nodes defined as a non-licensed API application	6

The following list provides details about the example fields:

Product
: The IBM Spectrum Protect product name.

Number of Client Devices
: The estimated number of client devices that are managed by the product. By default, only nodes on Microsoft Windows 7, Microsoft Windows XP Professional, and Apple systems are assumed to be client devices.

Number of Server Devices
: The estimated number of server devices that are managed by the product. By default, nodes on all platforms except for Microsoft Windows 7, Microsoft Windows XP Professional, and Apple systems are assumed to be server devices. This number also includes the server on which IBM Spectrum Protect is running.

PVU of Server Devices
: The estimated PVUs of all nodes that are connected as server devices.

Nodes earlier than Version 6.3 with no PVU information available at this time
: Devices that do not report processor information to the server.

Nodes at Version 6.3 or later with no PVU match
: Devices that do not report all required values or some values were reported as "Unknown".

Nodes classified by the administrator as "other-device"
: Nodes that are excluded from PVU counting by the administrator by using the update node roleoverride=other command.

Nodes defined as a non-licensed API application
: Nodes such as DB2® backup or custom API applications.

Example: Display detailed node information

Display information for individual nodes by specifying the detailed (d) value for the Format parameter. Issue the following command:

```
tsm: PATMOS_630> query pvuestimate f=d
```

Table 2. Node classifications for specific products

Product	Number of Client Devices	Number of Server Devices	PVU of Server Devices
IBM Spectrum Protect Extended Edition	1,000	905	90,500
- banode1	1		

Product	Number of Client Devices	Number of Server Devices	PVU of Server Devices
- banode2		1	200
- banode3	1		
- banode3		1	100
IBM Spectrum Protect for Storage Area Networks	50	10	1,000
- stagent1		1	50
- stagent2		1	100
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect for Mail	0	25	5,000
- mailnode1		1	200
- mailnode2		1	100
IBM Spectrum Protect for Databases	0	1,025	20,500
- dbnode1		1	200
- dbnode2		1	100
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5,000
- erpnode1		1	50
- erpnode2		1	100
IBM Spectrum Protect for System Backup and Recovery	0	0	0

Other Node Classifications	Number
Nodes earlier than Version 6.3 with no PVU information available at this time	10
- oldnode1	1
- oldnode2	1
- mailnote44	1
- erpnode66	1
Nodes at Version 6.3 or later with no PVU match	10
- badcitnode1	1
- badcitnode2	1
- mailnode23	1
- erpnode34	1
Nodes classified by administrator as "other-device"	8
- overriddennode1	1
- overriddennode2	1

Other Node Classifications	Number
- mailnode77	
Nodes defined as a non-licensed API application	6
- vendorapinode1	1
- vendorapinode2	1

Related commands

Table 3. Commands related to QUERY PVUESTIMATE

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.
QUERY LICENSE	Displays information about licenses and audits.
QUERY NODE	Displays partial or complete information about one or more clients.
REGISTER LICENSE	Registers a license with the IBM Spectrum Protect server.
REGISTER NODE	Defines a client node to the server and sets options for that user.
SET CPUINFOREFRESH	Specifies the number of days between client scans for workstation information used for PVU estimates.
SET LICENSEAUDITPERIOD	Specifies the number of days between automatic license audits.
UPDATE NODE	Changes the attributes that are associated with a client node.

QUERY RECOVERYMEDIA (Query recovery media)

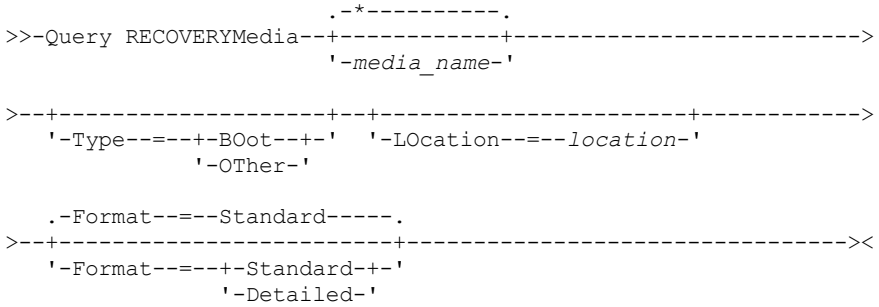
Use this command to display information about the media (for example, boot media) needed to recover a machine. Media are displayed in alphabetical order by name.

Remember: IBM Spectrum Protect™ does not use the information. It is available only to help you plan for the disaster recovery of client machines.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

media_name
: Specifies the name of the recovery media. You can use wildcard characters to specify the name. This parameter is optional. The default is all recovery media.

Type
: Specifies the type of media to be queried. This parameter is optional. If this parameter is not specified, all recovery media are queried. Possible values are:

  BOot
  : Only boot media are queried.

  OTher
  : All media other than boot media are queried.

LOcation
: Specifies the location of the recovery media to be queried. This parameter is optional. You can specify up to 255 characters. Enclose the description in quotation marks if it contains any blank characters.

Format
: Specifies how the information is displayed. This parameter is optional. Possible values are:

  Standard
  : Displays partial information. This is the default.

  Detailed
  : Displays all information.

Example: Display summary information for a specific recovery media

Display information for the recovery media named RECMED1. See Field descriptions for field descriptions.

```
query recoverymedia RECMED1

Recovery Media Name   Volume Names      Location          Machine Name
-------------------   ----------------  ----------------  ------------
RECMED1               vol1 vol2 vol3    IRONMOUNTAIN      MACH1
                       vol4
```

Example: Display detailed information for a specific recovery media

Display detailed information for the recovery media named RECMED1. See Field descriptions for field descriptions.

```
query recoverymedia RECMED1 format=detailed

Recovery Media Name: RECMED1
               Type: Boot
       Volume Names: vol1 vol2 vol3 vol4
           Location: IRONMOUNTAIN
        Description:
            Product:
Product Information:
       Machine Name: MACH1
```

Field descriptions

Recovery Media Name
: The name of the recovery media.

Type
: Whether the recovery media are boot media or another type of media. Possible values are:

  Boot
  : The recovery media are boot media.

  Other
  : The recovery media are not boot media.

Volume Names
: The set of volumes that contain the data needed to recover machines associated with this media.

Location
: Where the recovery media is stored.

Description

A description of the recovery media.

Product
: The product used to create the boot media.

Product Information
: Information about the product that created the boot media. This information may be needed for restoring the machine.

Machine Name
: The machines that are associated with this recovery media.

Related commands

Table 1. Commands related to QUERY RECOVERYMEDIA

Command	Description
DEFINE RECMEDMACHASSOCIATION	Associates recovery media with a machine.
DEFINE RECOVERYMEDIA	Defines the media required to recover a machine.
DELETE RECOVERYMEDIA	Deletes recovery media.
UPDATE RECOVERYMEDIA	Changes the attributes of recovery media.

QUERY REPLICATION (Query node replication processes)

Use this command to display information about running and ended node-replication processes.

Issue this command on the server that acts as a source for replicated data.

Important: You cannot display information about running replication processes for client nodes that are being converted from import and export operations to replication operations. The conversion process might run for a long time, but it occurs only once for a client node that is being converted.

By default, records about completed node-replication processes are retained for 30 calendar days. A *calendar day* consists of 24-hours, from midnight to midnight.

To display the retention period, issue the QUERY STATUS command. Check the value in the Replication Record Retention Period field. To change the retention period, issue the SET REPLRETENTION command.

Privilege class

Any administrator can issue this command.

Syntax

```
   .-DISplay--=--1--------------.
>--+----------------------------+------------------------------>
   '-DISplay--=--number_of_days-'

>--+-----------------------------------+------------------------>
   '-PROCessid--=--process_identifier-'

   .-STatus--=--ALl---------.  .-Format--=--Standard-----.
>--+----------------------+--+-------------------------+-----><
   '-STatus--=--+-ALl-----+-'  '-Format--=--+-Standard-+-'
                +-RUnning-+                 '-Detailed-'
                +-ENded---+
                '-FAiled--'
```

Notes:

1. Do not mix FSIDs (file space identifiers) and file space names in the same command.
2. Do not specify FSID if you use wildcard characters for the client node name.

Parameters

node_name (Required)

Specifies the name of the client node to be queried. You can use wildcard characters when you specify this name, with one exception. If the value of the NAMETYPE parameter is FSID, do not specify wildcard characters for the client node name. The FSID value indicates the file space identifier. File spaces with identical names can have different identifiers in different client nodes.

filespace_name or FSID

Specifies the name of the file space or the file space identifier (FSID) to be queried. A name or FSID is optional. If you do not specify a name or an FSID, all file spaces are queried.

filespace_name
: Specifies the name of the file space that has data to be queried. File space names are case-sensitive. To determine the correct capitalization for the file space, issue the QUERY FILESPACE command. Separate multiple names with commas with no intervening spaces. When you specify a name, you can use wildcard characters.

  A server that has clients with Unicode-enabled file spaces might have to convert the file space name. For example, the server might have to convert a name from the server code page to Unicode. For details, see the NAMETYPE parameter. If you do not specify a file space name, or if you specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

FSID
: Specifies the file space identifier for the file space to be queried. The server uses FSIDs to find the file spaces to replicate. To determine the FSID for a file space, issue the QUERY FILESPACE command. Separate multiple FSIDs with commas with no intervening spaces. If you specify an FSID, the value of the NAMETYPE parameter must be FSID.

NAMEType

Specifies how you want the server to interpret the file space names that you enter. You can use this parameter for IBM Spectrum Protect™ clients that are Unicode-enabled and that have Windows, Macintosh OS X, or NetWare operating systems.

Use this parameter only if you enter a partly qualified or fully qualified file space name. The default value is SERVER. You can specify one of the following values:

SERVER
: The server uses the server code page to interpret file space names.

UNIcode
: The server converts file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the characters in the name and the server code page. Conversion can fail if the string includes characters that are not available in the server code page. Conversion can also fail if the server cannot access system conversion routines.

FSID
The server interprets file space names by using their file space identifiers.

CODEType

Specifies the type of file spaces to be included in the query. The default value is BOTH, which means that file spaces are included regardless of code page type. Use this parameter only if you enter a single wildcard character for the file space name. You can specify one of the following values:

UNIcode
Include file spaces that are in Unicode only.
NONUNIcode
Include file spaces that are not in Unicode only.
BOTH
Include all file spaces regardless of code page type.

DISplay

Specifies the number of days of node replication history to display. The default value is 1, which displays information about running node replication processes and about processes that completed during the current calendar day. The maximum value is 9999.

You can specify a number that is the same as or less than the number of days that are specified as the retention period for the replication history records. If you specify a value that is more than the value of the replication retention period or more than the number of days that replication records are collected, the server displays only the number of replication history records that are available. For example, suppose that the replication retention period is 30 days and that the replication process is running for only 10 days. If you specify `DISPLAY=20`, only 10 days of replication history are displayed.

PROCessid
Specifies the node replication history that is associated with a particular process identified by the process identifier. This parameter is optional. If you do not specify this parameter, all processes are displayed for the number of days that are specified by the DISPLAY parameter.

Restarting the server can cause the server to reuse process IDs. Reuse of process IDs can result in duplicate process IDs for separate processes.

STatus
Specifies the status of the file spaces to query. This parameter is optional. The default value is ALL. You can specify one of the following values:

ALl
Specifies all file spaces that are replicating, file spaces that replicated successfully, and file spaces that did not finish replicating or replicated with errors.
RUnning
Specifies all file spaces that are replicating to the target replication server.
ENded
Specifies all file spaces that replicated successfully and file spaces that did not finish replicating or replicated with errors.
FAiled
Specifies all file spaces that did not finish replicating or replicated with errors.

Format
Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. You can specify one of the following values:

Standard
Specifies that partial information is displayed for node replication processes.
Detailed
Specifies that all available information for the node replication processes is displayed.

Example: Display information about replication processes for a file space

Display information about replication processes for a file space in client node PAYROLL. The file space identifier is 10.

```
query replication ironman
```

```
NodeName   Filespace   FSID   Start Time   End Time   Status  Phase
           Name
-------------------------------------------------------------------
IRONMAN    /space      2      02/08/11     02/08/11   Ended   None
                              21:44:19     21:48:14

query replication ironman format=detailed

                                    Node Name: IRONMAN
                               Filespace Name: /space
                                         FSID: 2
                                   Start Time: 02/08/11 21:44:19
                                     End Time: 02/08/11 21:48:14
                                       Status: Ended
                                Process Number: 4
                                      Command: replicate node ironman
                                        Phase: None
                           Process Running Time: 0 Day(s) 0 Hour(s)
                                                 4 Minute(s)
                                Completion State: Complete
                          Reason For Incompletion: None
                     Backup Last Update Date/Time:
                              Backup Target Server:
                   Backup Files Needing No Action: 0
                        Backup Files To Replicate: 0
                          Backup Files Replicated: 0
    Backup Files Not Replicated Due to Errors: 0
              Backup Files Not Yet Replicated: 0
                           Backup Files To Delete: 0
                             Backup Files Deleted: 0
       Backup Files Not Deleted Due To Errors: 0
                           Backup Files To Update: 0
                             Backup Files Updated: 0
       Backup Files Not Updated Due To Errors: 0
                Backup Bytes To Replicate (MB): 0
                  Backup Bytes Replicated (MB): 0
                 Backup Bytes Transferred (MB): 0
               Backup Bytes Not Replicated Due
                                  To Errors (MB): 0
         Backup Bytes Not Yet Replicated (MB): 0

                  Archive Last Update Date/Time: 02/08/11 21:48:14
                           Archive Target Server: NIGLINA
               Archive Files Needing No Action: 0
                    Archive Files To Replicate: 39,416
                      Archive Files Replicated: 39,206
   Archive Files Not Replicated Due to Errors: 210
             Archive Files Not Yet Replicated: 0
                       Archive Files To Delete: 0
                         Archive Files Deleted: 0
      Archive Files Not Deleted Due To Errors: 0
                       Archive Files To Update: 0
                         Archive Files Updated: 0


      Archive Files Not Updated Due To Errors: 0
               Archive Bytes To Replicate (MB): 4,335
                 Archive Bytes Replicated (MB): 4,335
                Archive Bytes Transferred (MB): 0
                  Archive Bytes Not Replicated
                              Due To Errors (MB): 0
        Archive Bytes Not Yet Replicated (MB): 0

           Space Managed Last Update Date/Time:
                Space Management Target Server:
         Space Managed Files Needing No Action: 0
              Space Managed Files To Replicate: 0
                Space Managed Files Replicated: 0
           Space Managed Files Not Replicated
                                Due to Errors: 0
        Space Managed Files Not Yet Replicated: 0
                  Space Managed Files To Delete: 0
                    Space Managed Files Deleted: 0
               Space Managed Files Not Deleted
                                Due To Errors: 0
```

```
                Space Managed Files To Update: 0
                  Space Managed Files Updated: 0
              Space Managed Files Not Updated
                                Due To Errors: 0
         Space Managed Bytes To Replicate (MB): 0
           Space Managed Bytes Replicated (MB): 0
          Space Managed Bytes Transferred (MB): 0
            Space Managed Bytes Not Replicated
                             Due To Errors (MB): 0
  Space Managed Bytes Not Yet Replicated (MB): 0
                Total Files Needing No Action: 0
                     Total Files To Replicate: 39,416
                       Total Files Replicated: 39,206
     Total Files Not Replicated Due To Errors: 210
               Total Files Not Yet Replicated: 0
                         Total Files To Delete: 0
                           Total Files Deleted: 0
        Total Files Not Deleted Due To Errors: 0
                         Total Files To Update: 0
                           Total Files Updated: 0
        Total Files Not Updated Due To Errors: 0
                 Total Bytes To Replicate (MB): 4,335
                   Total Bytes Replicated (MB): 4,335
                  Total Bytes Transferred (MB):
                    Total Bytes Not Replicated
                             Due to Errors (MB):
          Total Bytes Not Yet Replicated (MB):
                 Estimated Percentage Complete: 100
                      Estimated Time Remaining:
                  Estimated Time of Completion:
```

Field descriptions

Node Name
: The name of the client node whose data is displayed.

Filespace Name
: The name of the client file space whose data is displayed.

FSID
: The file space identifier.

Start Time
: The date and time that the node replication process started.

End Time
: The date and time that the node replication process ended.

Status
: The status of the node replication process. The following values are possible:

  Running
  : The process is active and is either searching for eligible data or sending data to the target replication server.

  Ended
  : The process ended or failed.

  Failed
  : The process failed.

Process Number
: The identifier for the node replication process.

  The same process number can have different start times. If a replication process starts and the server is restarted, the server begins assigning process numbers that begin with the number 1. Replication processes that start after a server restart can obtain process numbers that are already assigned to other replication processes in the replication history. To identify unique replication processes, use the start time.

Command
: The command that was issued to start the node replication process.

Phase
: The phase of a running node-replication process. The following phases are listed in the order in which they occur:

  Identifying

The node replication process started to identify data to be replicated, but data is not yet being sent to the target replication server.

Identifying and replicating
: The node replication process is identifying data to be replicated and transferring the data to the target replication server.

Replicating
: The node replication process identified the data and is transferring files to the target replication server.

None
: The node replication process is not running.

Process Running Time
: The running time of the node replication process.

Completion State
: The state of the node replication process. The following values are possible:

Complete
: The node replication process completed.

Incomplete
: The node replication process ended without running to completion. To determine the reason, check the value in the Reason for Incompletion field.

Reason for Incompletion
: The reason why the node replication process ended without completing. Possible values include *canceled* and *other*. The value *other* can indicate that the server was halted during replication or that the server failed.

Backup Last Update Date/Time
: The date and time that statistics for backup were last updated. The specified time is the time that the files in the file space were identified for replication or when each batch of files was sent to the target replication server.

Archive Last Update Date/Time
: The date and time that statistics for archive were last updated. The specified time is the time that the files in the file space were identified for replication or when each batch of files was sent to the target replication server.

Space Managed Last Update Date/Time
: The date and time that statistics for space-managed files were last updated. The specified time is the time that the files in the file space were identified for replication or when each batch of files was sent to the target replication server.

Backup Target Server
: The name of the target replication server for backup files.

Archive Target Server
: The name of the target replication server for archive files.

Space Management Target Server
: The name of the target replication server for space-managed files.

Backup Files Needing No Action
: The number of backup files in the file space that did not need to be replicated, updated, or deleted.

Archive Files Needing No Action
: The number of archive files in the file space that did not need to be replicated, updated, or deleted.

Space Managed Files Needing No Action
: The number of space-managed files in the file space that did not need to be replicated, updated, or deleted.

Backup Files To Replicate
: The number of backup files to replicate to the target replication server.

Archive Files To Replicate
: The number of archive files to replicate to the target replication server.

Space Managed Files To Replicate
: The number of space-managed files to replicate to the target replication server.

Backup Files Replicated
: The number of backup files that are replicated to the target replication server.

Archive Files Replicated
: The number of archive files that are replicated to the target replication server.

Space Managed Files Replicated
: The number of space-managed files that are replicated to the target replication server.

Backup Files Not Replicated Due To Errors
: The number of backup files that were not replicated to the target replication server because of errors.

Archive Files Not Replicated Due To Errors
: The number of archive files that were not replicated to the target replication server because of errors.

Space Managed Files Not Replicated Due To Errors
: The number of space-managed files that were not replicated to the target replication server because of errors.

Backup Files Not Yet Replicated
The number of backup files that are not yet replicated to the target replication server.
Archive Files Not Yet Replicated
The number of archive files that are not yet replicated to the target replication server.
Space Managed Files Not Yet Replicated
The number of space-managed files that are not yet replicated to the target replication server.
Backup Files To Delete
The number of backup files to be deleted on the target replication server.
Archive Files To Delete
The number of archive files to be deleted on the target replication server.
Space Managed Files To Delete
The number of space-managed files to be deleted on the target replication server.
Backup Files Deleted
The number of backup files that are deleted on the target replication server.
Archive Files Deleted
The number of archive files that are deleted on the target replication server.
Space Managed Files Deleted
The number of space-managed files that are deleted on the target replication server.
Backup Files Not Deleted Due To Errors
The number of backup files that were not deleted from the target replication server because of errors.
Archive Files Not Deleted Due To Errors
The number of archive files that were not deleted from the target replication server because of errors.
Space Managed Files Not Deleted Due To Errors
The number of space-managed files that were not deleted from the target replication server because of errors.
Backup Files To Update
The number of backup files to update on the target replication server. If the metadata of a file is changed, the changed fields are sent to the target replication server.
Archive Files To Update
The number of archive files to update on the target replication server. If the metadata of a file is changed, the changed fields are sent to the target replication server.
Space Managed Files To Update
The number of space-managed files to update on the target replication server. If the metadata of a file is changed, the changed fields are sent to the target replication server.
Backup Files Updated
The number of backup files that are updated on the target replication server.
Archive Files Updated
The number of archive files that are updated on the target replication server.
Space Managed Files Updated
The number of space-managed files that are updated on the target replication server.
Backup Files Not Updated Due To Errors
The number of backup files that were not updated on the target replication server because of errors.
Archive Files Not Updated Due To Errors
The number of archive files that were not updated on the target replication server because of errors.
Space Managed Files Not Updated Due To Errors
The number of space-managed files that were not updated on the target replication server because of errors.
Backup Bytes To Replicate (MB)
The number of backup bytes to replicate to the target replication server.
Archive Bytes To Replicate (MB)
The number of archive bytes to replicate to the target replication server.
Space Managed Bytes To Replicate (MB)
The number of space-managed bytes to replicate to the target replication server.
Backup Bytes Replicated (MB)
The number of backup bytes that are replicated to the target replication server.

If a file was stored in a deduplicated storage pool, the number of bytes in the stored file might be less than the number of bytes in the original file. This field represents the number of physical bytes in the original file.

Archive Bytes Replicated (MB)
The number of archive bytes that are replicated to the target replication server.

If a file was stored in a deduplicated storage pool, the number of bytes in the stored file might be less than the number of bytes in the original file. This field represents the number of physical bytes in the original file.

Space Managed Bytes Replicated (MB)
The number of space-managed bytes that are replicated to the target replication server.

If a file was stored in a deduplicated storage pool, the number of bytes in the stored file might be less than the number of bytes in the original file. This field represents the number of physical bytes in the original file.

Backup Bytes Transferred (MB)
The number of backup bytes that were sent to the target replication server.

The value in this field represents the actual number of file bytes sent to the target replication server. This value is calculated by subtracting the number of bytes not sent because of deduplication from the number of bytes to replicate.

Archive Bytes Transferred (MB)
The number of archive bytes that were sent to the target replication server.

The value in this field represents the actual number of file bytes sent to the target replication server. This value is calculated by subtracting the number of bytes not sent because of deduplication from the number of bytes to replicate.

Space Managed Bytes Transferred (MB)
The number of space-managed bytes that were sent to the target replication server.

The value in this field represents the actual number of file bytes sent to the target replication server. This value is calculated by subtracting the number of bytes not sent because of deduplication from the number of bytes to replicate.

Backup Bytes Not Replicated Due to Errors (MB)
The number of backup bytes that were not replicated to the target replication server because of errors.
Archive Bytes Not Replicated Due to Errors (MB)
The number of archive bytes that were not replicated to the target replication server because of errors.
Space Managed Bytes Not Replicated Due to Errors (MB)
The number of space-managed bytes that were not replicated to the target replication server because of errors.
Backup Bytes Not Yet Replicated (MB)
The number of backup bytes not yet replicated to the target replication server.
Archive Bytes Not Yet Replicated (MB)
The number of archive bytes not yet replicated to the target replication server.
Space Managed Bytes Not Yet Replicated (MB)
The number of space-managed bytes not yet replicated to the target replication server.
Total Files Needing No Action
The total number of files in the file space that did not need to be replicated, updated, or deleted.
Total Files To Replicate
The total number of files to replicate to the target replication server.
Total Files Replicated
The total number of files that are replicated to the target replication server.
Total Files Not Replicated Due To Errors
The total number of files that were not replicated because of errors.
Total files Not Yet Replicated
The total number of files that are not yet replicated to the target replication server.
Total Files To Delete
The total number of files that were deleted on the target replication server.
Total Files Deleted
The total number of files that are deleted on the target replication server.
Total Files Not Deleted Due to Errors
The total number of backup, archive, and space-managed files that were not deleted on the target replication server because of errors.
Total Files To Update
The total number of files to be updated on the target replication server. When the metadata of a file is changed, the changed fields are sent to the target replication server.
Total Files Updated
The total number of files that are updated on the target replication server.
Total Files Not Updated Due to Errors
The total number of backup, archive, and space-managed files that were not updated on the target replication server because of errors.
Total Bytes To Replicate (MB)
The total number of bytes to replicate to the target replication server.
Total Bytes Replicated (MB)

The total number of bytes that are replicated to the target server.

If a file was stored in a deduplicated storage pool, the number of bytes in the stored file might be less than the number of bytes in the original file. This field represents the number of physical bytes in the original file.

Total Bytes Transferred (MB)
The total number of bytes that were transferred to the target replication server.

For files stored in a deduplicated storage pool, the value in this field includes the number of bytes in the original file before duplicate extents were removed. If duplicate extents were already on the target replication server, the number of bytes in the original file is more than the number of bytes transferred.

Total Bytes Not Replicated Due to Errors (MB)
The total number of bytes that were skipped because the source replication server was unable to transfer them to the target replication server.

Total Bytes Not Yet Replicated (MB)
The total number of bytes not yet transferred to the target replication server.

Estimated Percentage Complete
The estimated completion percentage that is based on the number of bytes.

Estimated Time Remaining
The estimated time that remains before the node replication process is complete.

Estimated Time Of Completion
The estimated time when the node replication process ends.

Table 1. Commands related to QUERY REPLICATION

Command	Description
CANCEL REPLICATION	Cancels node replication processes.
QUERY ACTLOG	Displays messages from the server activity log.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY PROCESS	Displays information about background processes.
QUERY REPLNODE	Displays information about the replication status of a client node.
QUERY REPLRULE	Displays information about node replication rules.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET REPLRETENTION	Specifies the retention period for replication history records.

QUERY REPLNODE (Display information about replication status for a client node)

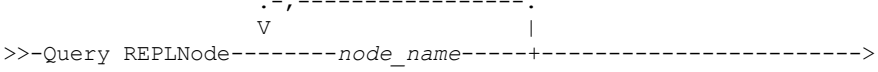
Use this command to display the number of files that are stored for each replicated file space. Information is displayed about file spaces for every client node that is configured for replication.

A client node is configured for replication if it is enabled or disabled.

Privilege class

Any administrator can issue this command.

Syntax



```
>--+--------------------+---------------------------------------><
   '-target_server_name-'
```

Parameters

node_name (Required)

Specifies the client node that owns the files about which you want information. You can specify one or more names. If you specify multiple names, separate the names with commas. Do not use intervening spaces. You can use wildcard characters to specify multiple names.

Information about client nodes that match the file criteria, but that are not configured for replication, is not displayed.

target_server_name

Specifies the name of the replication server to query for replication information. This parameter is optional. If you do not specify a value for this parameter, the server that is the default target for replicated data is queried.

As the value for this parameter, you can also specify a server that was formerly a target for replicated data.

The client nodes that are defined to a replication server can be the source or the target of replicated data. To determine whether a particular client node is sending or receiving data, issue the QUERY NODE command. Look for the value *Send* or *Receive* in the Replication Mode field of the output.

To display the name of the active target replication server, issue the QUERY STATUS command, and look for the name in the Target Replication Server field.

Example: List client node files on a source and a target replication server

The name of the client node is NODE1.

```
query replnode *

Node   Type   Filespace  FSID   Files on   Replication   Files on
Name           Name             Server     Server (1)   Server (1)
-------------------------------------------------------------------
NODE1  SpMg    /hmsmfs    1      1
NODE1  Bkup    /lspace2   2      27
NODE1  Arch    /lspace2   2      22         TGTSRV     22
NODE1  Bkup    /lspace    3      18,096
NODE1  Arch    /lspace    3      61,150     TGTSRV     61,150
NODE2
```

The number of files that are displayed for the replication servers might be different for the following reasons:

- The output of the QUERY REPLNODE command displays the number of files obtained from the occupancy table. The occupancy table contains only files that have a length greater than zero. Files that have a length of 0 and have been replicated are not reflected in this output.
- If only active data is replicated to the target server, the number of files that are displayed for the source server will be larger than the number of files that are displayed on the target server. The reason for the difference is that the source replication server has both active and inactive data, and the target server has only active data.
- A client node might have data that was exported from the source replication server and imported to the target replication server. If that data was synchronized and if the client node also stored data to the target replication server, then the number of files on the target replication server will be greater than the number of files stored as a result of export-and-import operations and replication.
- When you replicate node data from a source server prior to version 7.1, to a target server at version 7.1 or later, files that are larger than 10 GB are split in to smaller files if the SPLITLARGEOBJECTS parameter for the node definition is set to `Yes`. Each of these split files are counted on the target server.

Field descriptions

Node Name

The name of the client node that owns the files.

Type

The type of data. If this field is blank, the client node is configured for replication, but it does not have data on the replication server. In the example output, NODE2 is configured for replication, but it does not have backup, archive, or space-managed data.

The following values are possible:

Arch
: Archive data

Bkup
: Backup data

SpMg
: Data that was migrated by IBM Spectrum Protect™ for Space Management clients

Filespace Name

The name of the file space that belongs to the node.

If this field is blank, the client node is configured for replication, but it does not have data on the replication server.

File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

FSID
: The file space identifier for the file space. The server assigns a unique FSID when a file space is initially stored on the server. If this field is blank, the client node is configured for replication, but it does not have data on the replication server.

Files on Server
: The number of backup, archive, and space-managed files on the server on which this command is issued. If this field is blank, the client node is configured for replication, but it does not have data on the replication server.

Replication Server (1)
: The name of the replication server that is being queried for information. If this field is blank, one or more of the following conditions might exist:

- The file space of the node on the replication server where the command was issued does not have any data.
- The client node is not defined on replication server (1).
- The client node is defined on replication server (1), but the node is not configured for replication.
- The corresponding file space on replication server (1) does not have data or the file space is not defined.

Files on Server (1)
: The number of files for the data type that are stored on the target replication server. This field can be blank. If it is, one or more of the following conditions might exist:

- Replication server (1) does not have any data.
- The client node is not defined on replication server (1).
- The client node is defined on replication server (1), but the node is not configured for replication.
- The corresponding file space on replication server (1) does not have data or the file space is not defined.

Related commands

Table 1. Commands related to QUERY REPLNODE

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.

Command	Description
QUERY REPLRULE	Displays information about node replication rules.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
UPDATE REPLRULE	Enables or disables replication rules.

QUERY REPLRULE (Query replication rules)

Use this command to display information about replication rules.

Issue this command on the server that acts as a source for replicated data.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*-----------------------------.
>>-Query REPLRule--+-------------------------------+-----------><
                    '-+-ALL_DATA------------------+-'
                      +-ACTIVE_DATA---------------+
                      +-ALL_DATA_HIGH_PRIORITY----+
                      '-ACTIVE_DATA_HIGH_PRIORITY-'
```

Privilege class

Any administrator can issue this command.

Parameters

rule_name
: Specifies the name of the replication rule that you want to display information about. This parameter is optional. You can use wildcard characters to specify one or more rules. If you do not specify this parameter, information about all rules is displayed in the query output. You can specify the following values:

  ALL_DATA
  : Displays information about the ALL_DATA replication rule. This rule replicates backup, archive, or space-managed data. The data is replicated with a normal priority.

  ACTIVE_DATA
  : Displays information about ACTIVE_DATA replication rule. This rule replicates only active backup data. The data is replicated with a normal priority. This rule is not valid for archive or space-managed data.
    Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

    - When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
    - When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
    - When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

    If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

  ALL_DATA_HIGH_PRIORITY
  : Displays information about the ALL_DATA_HIGH_PRIORITY rule. This rule replicates backup, archive, or space-managed data. The data is replicated with a normal priority. In a replication process, high-priority data is replicated before normal-priority data.

  ACTIVE_DATA_HIGH_PRIORITY
  : Displays information about the ACTIVE_DATA_HIGH_PRIORITY rule.

    This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

Example: Display information about a server replication rule

The name of the rule is ALL_DATA_HIGH_PRIORITY

```
query replrule all_data_high_priority

Replication Rule Name: ALL_DATA_HIGH_PRIORITY
Target Replication Server:
Active Only: No
Enabled: Yes
```

Field descriptions

Replication Rule Name
: Specifies the name of the rule that was queried.

Target Replication Server
: Specifies the name of the target replication server.

Active Only
: Specifies whether the rule applies only to active backup data. The following values are possible:

  Yes
  : Specifies that only active backup data is replicated for file spaces to which this rule is assigned.

  No
  : Specifies that all backup data is replicated for file spaces to which this rule is assigned.

Enabled
: Specifies whether the rule is enabled or disabled. The following values are possible:

  Yes
  : Specifies that the rule is enabled for replication. Data in file spaces to which the rule is assigned is replicated.

  No
  : Specifies that the rule is not enabled for replication. Data in file spaces to which the rule is assigned is not replicated.

Related commands

Table 1. Commands related to QUERY REPLRULE

Command	Description
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLNODE	Displays information about the replication status of a client node.
UPDATE REPLRULE	Enables or disables replication rules.

QUERY REPLSERVER (Query a replication server)

Use this command to view information about all replication servers that are known server. The output from this command includes server information for the server from which the command was issued. The command indicates whether a replication server definition is deleted as a result of a REMOVE REPLSERVER command.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*-----------.
>>-Query REPLServer--+-------------+--------------------------><
                    '-server_name-'
```

Example: Display summary statistics about all replicating servers

Display information about the replicating server. Issue the command from either the source or the target replication server:

```
query replserver *

Replication Globally Unique ID: 4d.83.fc.30.67.c1.11.e1.b8.
                                      40.f0.de.f1.5e.f1.89
                   Server Name: Server1
               Last Replication:
                      Heartbeat:
   Failover High Level Address: server1.example.com
      Failover TCP Port Number: 1500
      Failover SSL Port Number: 1542
          Deletion in Progress: No
           Dissimilar Policies:

Replication Globally Unique ID: 91.0f.ef.90.5c.cc.11.e1.ae.
                                34.08.00.27.00.58.dc
                   Server Name: DRServer1
               Last Replication: 06/30/2012 08:16:30 PM
                      Heartbeat: 07/09/2012 22:15:22 PM
  Fail over High Level Address: drserver1.example.com
      Failover TCP Port Number: 1500
      Failover SSL Port Number: 1542
          Deletion in Progress: No
           Dissimilar Policies: On

Replication Globally Unique ID: 90.4f.53.b0.8e.cb.11.e3.a8.
                                2f.00.14.5e.55.b3.67
                   Server Name: DRSERVER2
               Last Replication: 04/01/14   12:38:28
                      Heartbeat: 05/29/14   11:15:44
   Failover High Level Address: drserver2.example.com
      Failover TCP Port Number: 1500
      Failover SSL Port Number:
          Deletion in Progress: No
           Dissimilar Policies: Off
```

Example: Display summary statistics about a specific replicating server

Display information about the replicating server DRServer1. Issue the command from either the source or the target replication server:

```
query replserver drserver1

Replication Globally Unique ID: 91.0f.ef.90.5c.cc.11.e1.ae.
                                      34.08.00.27.00.58.dc
                   Server Name: DRServer1
               Last Replication: 06/30/2012 08:16:30 PM
                      Heartbeat: 07/09/2012 22:15:22 PM
  Fail over High Level Address: drserver1.example.com
      Failover TCP Port Number: 1500
      Failover SSL Port Number: 1542
          Deletion in Progress: No
           Dissimilar Policies: On
```

Parameters

server_name
: Specifies the name of the replication server to be queried. You can use wildcard characters to specify this name. All matching servers are queried. If you do not specify a value for this parameter, all servers are queried. The parameter is optional.

Field descriptions

Replication Globally Unique ID
: The unique identifier for the IBM Spectrum Protect™ server. The values for the Replication Globally Unique ID are created when a server is first used in a replication process.
: Tip: The ID listed in the Replication Globally Unique ID field is not the same value as the value for the ID listed in the Machine Globally Unique ID field that is shown in the QUERY STATUS command.

Server Name

The name of the replication server.

Last Replication
: The date of the last replication process that used the server.

Heartbeat
: The last time that the server completed a successful test communication session.

Failover TCP Port Number
: The active Transmission Control Protocol (TCP) client port on the replication server that is used for client connections. If the client is configured for TCP, the port is used to connect to the failover server.

Failover SSL Port Number
: The active Secure Sockets Layer (SSL) port on the replication server that is used for client connections. If the client is configured for SSL, the port is used to connect to the failover server.

Failover High Level Address
: The high-level address that the client uses to connect to the replication server during failover.

Deletion in Progress
: Specifies whether a REMOVE REPLSERVER command was issued for this replication server and is still in progress. The following values are possible:

  Yes
  : The deletion of the replication server is in progress.

  No
  : The deletion of the replication server is not in progress.

Dissimilar Policies
: Specifies whether the policies that are defined on the target replication server are enabled. The following values are possible:

  On
  : The policies on the target replication server manage replicated client-node data.

  Off
  : The policies on the source replication server manage replicated client-node data.

Related commands

Table 1. Commands related to QUERY REPLSERVER

Command	Description
REMOVE REPLNODE (Remove a client node from replication)	Removes a node from replication.
REMOVE REPLSERVER (Remove a replication server)	Removes a server from replication.

QUERY REQUEST (Query one or more pending mount requests)

Use the QUERY REQUEST command to show information about one or more pending mount requests. The server makes requests for the administrator to complete an action, like inserting a tape volume in a library after a CHECKIN LIBVOL is issued.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query REQuest--+----------------+--------------------------><
                  '-request_number-'
```

Parameters

request_number
: Specifies the identification number of the pending mount request. This parameter is optional. The default is all pending mount requests.

Example: List all pending mount requests

Display information about all pending mount requests after a CHECKIN LIBVOL is issued.

```
query request
```

Output for a manual Library

AIX

```
ANR8352I Requests outstanding:
ANR8326I 001: Mount 8MM volume EXP001 R/W
in drive 8MM.1 (/dev/mt0) of library
MANUALLIB within 60 minute(s).
```

Linux

```
ANR8352I Requests outstanding:
ANR8326I 001: Mount 8MM volume EXP001 R/W
in drive 8MM.1 (/dev/mt0) of library
MANUALLIB within 60 minute(s).
```

Windows

```
ANR8352I Requests outstanding:
ANR8326I 001: Mount GENERICTAPE volume EXP001 R/W
in drive 8MM.1 (mt3.0.0.0) of library
MANUALLIB within 60 minute(s).
```

Output for an automated Library

AIX | Windows

```
ANR8352I Requests outstanding:
ANR8306I 001: Insert LTO volume 133540L5 R/W into the slot with
 element number 31 of library LTOLIB within 60 minutes; issue
 'REPLY' along with the request ID when ready.
```

Linux

```
ANR8352I Requests outstanding:
ANR8306I 001: Insert 3590 volume 133540 R/W into the slot with element
 number 31 of library 3590LIB within 60 minutes; issue 'REPLY'
 along with the request ID when ready.
```

Related commands

Table 1. Related commands for QUERY REQUEST

Command	Description
CANCEL REQUEST	Cancels pending volume mount requests.
REPLY	Allows a request to continue processing.

QUERY RESTORE (Query restartable restore sessions)

Use this command to display information about the restartable restore sessions.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query--RESTore--+-----------+--+-----------------+----------->
                   '-node_name-'  '-file_space_name-'

   .-Format--=--Standard-----.  .-NAMEType--=--SERVER------.
```

```
>--+-------------------------+--+-------------------------+---><
   '-Format--=--+-Standard-+-'  '-NAMEType--=--+-SERVER--+-'
                '-Detailed-'                   +-UNIcode-+
                                               '-FSID----'
```

Parameters

node_name
: Specifies the client node to be queried. This parameter is optional. If you do not specify a value, all client nodes with restartable restore sessions are displayed. You must specify a value for this parameter if you specify a file space name.

file_space_name
: Specifies the file space to be queried. This parameter is optional. If you do not specify a value, all file spaces are matched for the specified node.

  For a server that has clients with support for Unicode, you may need to have the server convert the file space name that you enter. For example, you may need to have the server convert the name you enter from the server's code page to Unicode. See the NAMETYPE parameter for details.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

NAMEType
: Specify how you want the server to interpret the file space names that you enter. This parameter is useful when the server has clients with support for Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect™ clients using Windows, Macintosh OS 9, Macintosh OS X, and NetWare operating systems.

  Use this parameter only when you enter a partly or fully qualified file space name. The default value is SERVER. Possible values are:

  SERVER
  : The server uses the server's code page to interpret the file space names.

  UNIcode
  : The server converts the file space name entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server has a problem accessing system conversion routines.

  FSID
  : The server interprets the file space names as their file space IDs (FSIDs).

Example: Display a restartable restore session on a specific client node

Display detailed information about client node JAMES associated with file space DRIVE_F_R. See Field descriptions for field descriptions.

```
query restore james drive_f_r format=detailed

    Sess Number: -1
  Restore State: Restartable
Elapsed Minutes: 2
      Node Name: JAMES
           FSID: 1
 Filespace Name: DRIVE_F_R:
      File Spec: /RESTORE/TESTDIRF\\
```

Field descriptions

Sess Number
: Specifies the session number for the restartable restore session. The number for active restore sessions is the same number displayed on the QUERY SESSION command. For restore sessions in the restartable state, a negative number is

displayed for the session number. Any session number displayed in the QUERY RESTORE output may be specified from the QUERY RESTORE output.

Restore State

- Active: Specifies the restore session is actively restoring files to the client.
- Restartable: Specifies the restore session failed and can be restarted from where it left off.

Elapsed Minutes
Specifies the number of minutes since the restore session started. Any restartable restore session with an elapsed time greater than the RESTOREINTERVAL server option can be automatically deleted from the database when needed or during expiration processing. If the elapsed time is less than the RESTOREINTERVAL, you can delete this entry (and unlock the filespace) only by issuing the CANCEL RESTORE command lowering the RESTOREINTERVAL value.

Node Name
Specifies the node associated with the restartable restore session.

FSID
Specifies the file space ID of the file space.

Filespace Name
Specifies the file space associated with the restartable restore session.

File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

File Spec
Specifies the file specification used on the restore operation. The same file specification must be specified if a failed restore operation is to be restarted from where it stopped.

Related commands

Table 1. Commands related to QUERY RESTORE

Command	Description
CANCEL RESTORE	Cancels a restartable restore session.

QUERY RPFCONTENT (Query recovery plan file contents stored on a target server)

Use this command to display the contents of a recovery plan file stored on a target server (that is, when the DEVCLASS parameter was specified on the PREPARE command). You can issue this command from either the server that created the file (the source server) or the server that stores the recovery plan file (the target server). You cannot issue this command from the server console.

The output may be delayed if the file is on tape.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Query RPFContent--plan_file_name----------------------------->

>--+-DEVclass--=--device_class_name-+-------------------------><
   '-NODEName--=--node_name---------'
```

Parameters

plan_file_name (Required)
Specifies the name of the recovery plan file to be queried. The format of the file name is servername.yyyymmdd.hhmmss. To see the names of existing files, issue the QUERY RPFILE command.

DEVclass
Specifies the name of the device class used to create the recovery plan file. Wildcard characters are not allowed.
Specify this parameter when:

- You want to display the contents of the recovery plan file that was created for this server.
- You are issuing this command to the same server on which the PREPARE command was issued (the source server).
- The specified device class name was used on the PREPARE command that created the recovery plan file.

NODEName
Specifies the node name, registered on the target server, of the source server that created the recovery plan file. Wildcard characters are not allowed.
Specify this parameter when:

- You want to display the contents of the recovery plan file that was stored on this server.
- You are issuing this command to the server that was the target of the PREPARE command that created the recovery plan file.
- The specified node name is registered to this server with a node type of SERVER.
- The IBM Spectrum Protect™ server that created the recovery plan file is not available.

Example: Display the source server recovery plan

On the source server, display the contents of a recovery plan file that was created for this server on March 19, 1998, at 6:10 A.M. The PREPARE command specifies the device class REMOTE. The output of this command is the entire contents of the recovery plan file.

```
query rpfcontent branch1.19980319.061000 devclass=remote
```

Example: Display the target server recovery plan

On the target server, display the contents of a recovery plan file that was stored in this server on March 19, 1998, at 6:10 A.M. The server that created the file is registered on the target server as a node named POLARIS with a node type of SERVER. The output of this command is the entire contents of the recovery plan file.

```
query rpfcontent branch1.19980319.061000 nodename=polaris
```

Related commands

Table 1. Commands related to QUERY RPFCONTENT

Command	Description
PREPARE	Creates a recovery plan file.
QUERY RPFILE	Displays information about recovery plan files.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.

Related information:
Disaster recovery plan file

QUERY RPFILE (Query recovery plan file information stored on a target server)

Use this command to display information about recovery plan files stored on a target server. You can issue this command from either the server that created the file (the source server) or the server that stores the recovery plan file (the target server).

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query RPFile--+-DEVclass--=--device_class_name-+-------------->
                 '-NODEName--=--node_name---------'

   .-Source--=--DBBackup-------.  .-Format--=--Standard-----.
>--+---------------------------+--+-------------------------+--><
   '-Source--=--+-DBBackup---+-'  '-Format--=--+-Standard-+-'
                '-DBSnapshot-'                 '-Detailed-'
```

Parameters

DEVclass
: Specifies the name of the device class that was used to create the recovery plan files. Use this parameter when logged on to the server that created the recovery plan file. You can use wildcard characters in the device class name. All recovery plan files that are created with the device class specified are included in the query.

NODEName
: Specifies the node name, registered on the target server, of the source server that created the recovery plan files. Use this parameter when logged on to the target server. You can use this parameter when the source server is not available. You can use wildcard characters to specify the node name. All file objects that are stored with the node name specified are included in this query.

Source
: Specifies the type of database backup that was specified when the recovery plan file was prepared. This parameter is optional. The default is DBBACKUP. Possible values are:

  DBBackup
  : The recovery plan file was prepared with full and incremental database backups specified.

  DBSnapshot
  : The recovery plan file was prepared with snapshot database backups specified.

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Displays partial information for the recovery plan file.

  Detailed
  : Displays all information for the recovery plan file.

Example: Display detailed information about the recovery plans

Display recovery plan files that were created for this server using the specified device class. See Field descriptions for field descriptions.

```
query rpfile devclass=* format=detailed
```

```
    Recovery Plan File Name: ALASKA.20000406.170423
                  Node Name: BRANCH1
        Device Class Name: REMOTE
    Recovery Plan File Type: RPFILE
          Mgmt Class Name: STANDARD
    Recovery Plan File Size: 16,255 Bytes
        Marked for Deletion: Yes
              Deletion Date: 06/12/2000 13:05:31

    Recovery Plan File Name: ALASKA.20000407.170845
                  Node Name: BRANCH1
        Device Class Name: REMOTE
    Recovery Plan File Type: RPFSNAPSHOT
          Mgmt Class Name: STANDARD
    Recovery Plan File Size: 16,425 Bytes
        Marked for Deletion: No
              Deletion Date:
```

Example: Display a list of recovery plans for a specific node name

Display a list of all recovery plan file objects that are stored with the specified node name (TYPE=SERVER). See Field descriptions for field descriptions.

```
query rpfile nodename=branch1

    Recovery Plan File Name       Node Name       Device Class Name
    -----------------------       ---------       -----------------
     ALASKA.19980406.170423         BRANCH1         REMOTE
     ALASKA.19980407.170845         BRANCH1         REMOTE
```

Field descriptions

Recovery Plan File Name
: The recovery plan file name.

Node Name
: The node name that is registered with the target server and used to store the recovery plan file objects.

Device Class Name
: The device class name that is defined in the source server and used to create the recovery plan files.

Recovery Plan File Type
: The type of recovery plan file:

  RPFILE
  : The plan assumes full plus incremental database backups.

  RPFSNAPSHOT
  : The plan assumes snapshot database backups.

Mgmt Class Name
: The management class name that the recovery plan file is associated with in the target server.

Recovery Plan File Size
: Estimated size of the recovery plan file object on the target server.

Marked For Deletion
: Whether the object that contains the recovery plan file has been deleted from the source server and marked for deletion on the target server if the grace period has not expired. Possible values are:

  Yes
  : The object is marked for deletion.

  No
  : The object is not marked for deletion.

Deletion Date
: Date that the object has been deleted from the source server and marked for deletion on the target server. This field is blank if the object has not been marked for deletion.

Related commands

Table 1. Commands related to QUERY RPFILE

Command	Description
PREPARE	Creates a recovery plan file.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
QUERY RPFCONTENT	Displays the contents of a recovery plan file.

QUERY SAN (Query the devices on the SAN)

Use this command to obtain information about devices that can be detected on a storage area network (SAN) so that you can configure IBM Spectrum Protect™ for LAN-free data movement.

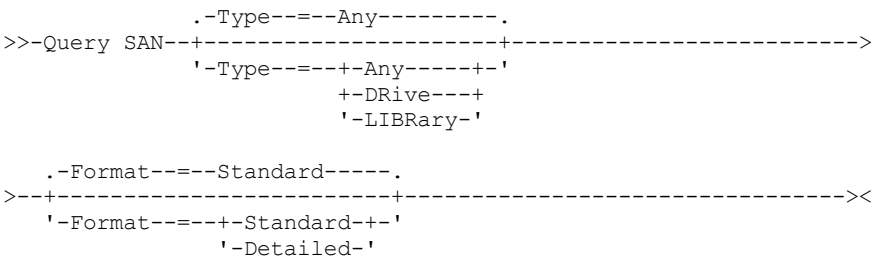
AIX The QUERY SAN command requires the libhbaapi.a that supports SNIA common Host Bus Adapter (HBA) API. With this library object, IBM Spectrum Protect can call the hbaapi functions that are specified in the SNIA common HBAAPI standard.

Windows The QUERY SAN command requires the hbaapi.dll that supports SNIA common Host Bus Adapter (HBA) API. With this library object, IBM Spectrum Protect can call the hbaapi functions that are specified in the SNIA common HBAAPI standard.
Linux The QUERY SAN command requires the libhaapi.so that supports SNIA common Host Bus Adapter (HBA) API. With this library object, IBM Spectrum Protect can call the hbaapi functions that are specified in the SNIA common HBAAPI standard.
The QUERY SAN command might not show all the devices if the SANDISCOVERY server option is not set to ON.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

Type
: Specifies the type of device that is displayed. This parameter is optional. The default value is Any. Possible values are:

  Any
  : Specifies that any device detected on the SAN is displayed.

  DRive
  : Specifies that only drive devices are displayed.

  LIBRary
  : Specifies that only library devices are displayed.

Format
: Specifies the type of information that is displayed. This parameter is optional. The default value is Standard. Possible values are:

  Standard
  : Specifies that the information displayed is summarized.

  Detailed
  : Specifies that complete information is displayed.

  Tip: The output might not display the serial number of the device. If this happens, look on the back of the device or contact the manufacturer of the device.

Example: List drive devices

Display summary information for drive devices on a SAN. See Field descriptions for field descriptions.

```
query san type=drive
```

```
Device Type      Vendor        Product     Serial           Device
-------------    ----------    ---------   ---------        ----------
LIBRARY          STK           L180        MPC01000128      /dev/smc1
DRIVE            STK           9840D       331001017229     /dev/rmt3
DRIVE            Quantum       DLT4000     JF62806275       /dev/rmt4
DRIVE            Quantum       DLT4000     JP73213185       /dev/rmt5
DRIVE            STK           9840D       331000028779     /dev/rmt6
```

Example: Display drive device information

Display detailed information for all drive devices on a SAN. See Field descriptions for field descriptions.

```
query san type=drive format=detailed

                     Device Type:    DRIVE
                          Vendor:    IBM
                         Product:    03570B02
                   Serial Number:
                          Device:    mt10.2.0.3
                      DataMover:    No
                       Node WWN:    5005076206039E05
                       Port WWN:    5005076206439E05
                            LUN:    0
                      SCSI Port:    3
                       SCSI Bus:    0
                    SCSI Target:    10
```

Field descriptions

Device Type
: The type of device that is being displayed.

Vendor
: The name of the device's vendor.

Product
: The name of the product that is assigned by the vendor.

Serial Number
: The serial number of the device.

Device
: The device special file name.

Data Mover
: Whether the device is a data mover.

Node WWN
: The worldwide name for the device.

Port WWN
: The worldwide name for the device, which is specific to the port that the device is connected to.

LUN
: The Logical Unit Number of the device.

SCSI Port
: The port of the Fibre Channel (or SCSI) Host Bus Adapter.

SCSI Bus
: The bus of the Host Bus Adapter card.

SCSI Target
: The target number of the device.

Related commands

Table 1. Commands related to QUERY SAN

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.

QUERY SCHEDULE (Query schedules)

Use this command to display information about one or more schedules.

The QUERY SCHEDULE command takes two forms, depending on whether the schedule applies to client operations or administrative commands. The syntax and parameters for each operation are defined separately. Some options in the query display will be blank depending on whether the schedule style is classic or enhanced.

Table 1. Commands related to QUERY SCHEDULE

Command	Description

Command	Description
COPY SCHEDULE	Creates a copy of a schedule.
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
UPDATE SCHEDULE	Changes the attributes of a schedule.

- QUERY SCHEDULE (Query client schedules)
  Use this command to display information about one or more client schedules.
- QUERY SCHEDULE (Query an administrative schedule)
  Use this command to display information about one or more administrative schedules.

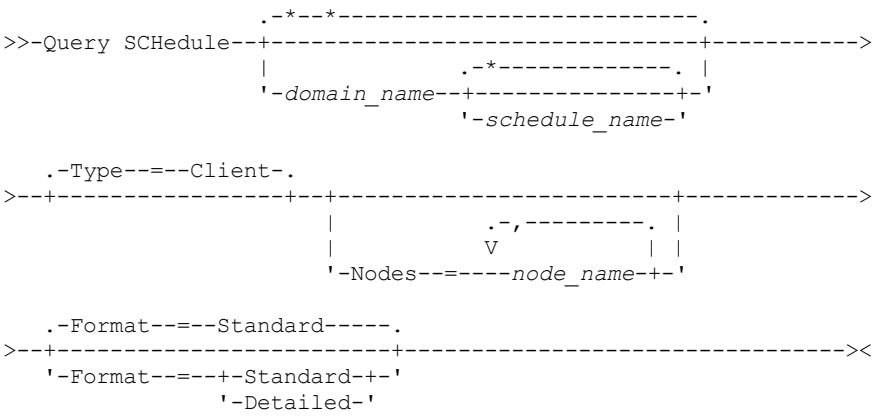
QUERY SCHEDULE (Query client schedules)

Use this command to display information about one or more client schedules.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

domain_name
: Specifies the name of the policy domain to which the schedule belongs. You can use a wildcard character to specify this name. If you specify a domain name, you do not have to specify a schedule name.

schedule_name
: Specifies the name of the schedule that belongs to the specified policy domain. You can use a wildcard character to specify this name. If you specify a schedule name, you must also specify a policy domain name.

Type=Client
: Specifies that the query displays client schedules. This parameter is optional. The default is CLIENT.

Nodes
: Specifies the name of one or more client nodes that are associated with the schedules to be displayed. This parameter is optional. You can use a wildcard character to specify client nodes. If you do not specify a client name, all schedules matching the DOMAINNAME and SCHEDULENAME parameters are displayed. You can specify multiple client nodes by separating the names with commas and no intervening spaces.

Format
: Specifies how information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the schedules.

  Detailed
  : Specifies that detailed information is displayed for the schedules.

The standard format displays a blank in the period column and an asterisk in the day column for enhanced schedules. To display complete information about an enhanced schedule, issue FORMAT=DETAILED.

Example: List schedules for a specific policy domain

Display all schedules that belong to the EMPLOYEE_RECORDS policy domain. See Field descriptions: Schedules for a specific policy domain for field descriptions.

```
query schedule employee_records
```

The standard format displays a blank in the period column and an asterisk in the day column for enhanced schedules. To display complete information about an enhanced schedule, issue FORMAT=DETAILED.

```
Domain   * Schedule Name   Action Start       Duration Period Day
                                Date/Time
-------- - --------------  ------ ----------  -------- ------ ---
EMPLOY     WEEKLY_BACKUP   Inc Bk 2004.06.04  1 H      1 D    Any
EE_RE-                            17.04.20
CORDS
EMPLOY-    EMPLOYEE_BACKUP Inc Bk 2004.06.04  1 H             (*)
EE_RE-                            17.04.20
CORDS
```

Field descriptions: Schedules for a specific policy domain

Domain
: Specifies the name of the policy domain to which the specified schedule belongs.

* (Asterisk)
: Specifies whether the corresponding schedule has expired. If there is an asterisk in this column, the corresponding schedule has expired.

Schedule Name
: Specifies the name of the schedule.

Action
: Specifies the action that occurs when this schedule is processed.

Start Date/Time
: Specifies the initial starting date and time for this schedule.

Duration
: Specifies the length of the startup window for this schedule.

Period
: Specifies the time between startup windows (assuming DAYOFWEEK=ANY). The column is blank for enhanced schedules.

Day
: Specifies the day of the week on which the startup windows for the schedule begin. The column contains an asterisk for enhanced schedules.

Example: Display detailed client schedules

From a managed server, display detailed information about client schedules. See Field descriptions: Detailed client schedules for field descriptions.

```
query schedule * type=client format=detailed

            Policy Domain Name: ADMIN_RECORDS
                 Schedule Name: ADMIN_BACKUP
                   Description:
                        Action: Backup
                     Subaction: vApp
                       Options:
                       Objects:
                      Priority: 5
                Start Date/Time: 04/06/2013 17.04.20
                      Duration: 1 Hour(s)
    Maximum Run Time (Minutes): 0
                Schedule Style: Classic
                        Period: 1 Day(s)
                   Day of Week: Any
                         Month:
                  Day of Month:
```

```
                Week of Month:
                   Expiration:
Last Update by (administrator): $$CONFIG_MANAGER$$
         Last Update Date/Time: 04/06/2013 17.51.49
              Managing profile: ADMIN_INFO

            Policy Domain Name: EMPLOYEE_RECORDS
                 Schedule Name: EMPLOYEE_BACKUP
                   Description:
                        Action: Incremental
                     Subaction:
                       Options:
                       Objects:
                      Priority: 5
                Start Date/Time: 2004.06.04 17.04.33
                      Duration: 1 Hour(s)
    Maximum Run Time (Minutes): 0
                Schedule Style: Enhanced
                        Period:
                   Day of Week: Any
                         Month: Mar,Jun,Nov
                  Day of Month: -14,14,22
                Week of Month: Last
                   Expiration:
Last Update by (administrator): $$CONFIG_MANAGER$$
         Last Update Date/Time: 2004.06.04 17.18.30
              Managing profile: EMPLOYEE
```

Field descriptions: Detailed client schedules

Policy Domain Name
: Specifies the name of the policy domain.

Schedule Name
: Specifies the name of the schedule.

Description
: Specifies the description of the schedule.

Action
: Specifies the type of action that occurs when this schedule is run. See the DEFINE SCHEDULE command for a listing of actions.

Subaction
: Specifies that the type of operation identified by the ACTION parameter is to be scheduled. See the DEFINE SCHEDULE command for a listing of subactions.

Options
: Specifies the options that are supplied to the DSMC command when the schedule is run.

Objects
: Specifies the objects for which the specified action is performed.

Priority
: Specifies the priority value for the schedule.

Start Date/Time
: Specifies the initial starting date and time for the schedule.

Duration
: Specifies the length of the startup window for the schedule.

Maximum Run Time (Minutes)
: Specifies the number of minutes during which all client sessions that are started by the scheduled operation should be completed. If sessions are still running after the maximum run time, the server issues a warning message, but the sessions continue to run.

Schedule Style
: Specifies whether classic or enhanced schedule rules are used.

Period
: Specifies the time between startup windows (assuming DAYOFWEEK=ANY). This is not displayed for enhanced syntax schedules.

Day of Week
: Specifies the day of the week on which the startup windows for the schedule begin. Using a standard format displays an asterisk in the day of week field for enhanced schedules.

Month
: Specifies the months during which the schedule will run. This is not displayed for classic syntax schedules.

Day of Month
: Specifies the days of the month during which the schedule will run. This is not displayed for classic syntax schedules.

Week of Month
: Specifies the weeks (first, second, third, fourth, or last) of the month during which the schedule will run. This is not displayed for classic syntax schedules.

Expiration
: Specifies the date and time on which this schedule expires. If this column is blank, the schedule does not expire.

Last Update by (administrator)
: Specifies the name of the administrator that most recently updated the schedule. If this field contains a $$CONFIG_MANAGER$$, the schedule is associated with a domain that is managed by the configuration manager.

Last Update Date/Time
: Specifies the last date and time the schedule was last updated.

Managing Profile
: Specifies the profile or profiles to which the managed server subscribed to get the definition of this schedule.

QUERY SCHEDULE (Query an administrative schedule)

Use this command to display information about one or more administrative schedules.

Privilege class

Any administrator can issue this command.

Syntax

```
                    .-*-------------.
>>-Query SCHedule--+---------------+--Type--=--Administrative--->
                    '-schedule_name-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

schedule_name
: Specifies the name of the schedule to be queried. You can use a wildcard character to specify this name.

Type=Administrative (Required)
: Specifies that the query displays administrative command schedules.

Format
: Specifies how information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the schedules.

  Detailed
  : Specifies that detailed information is displayed for the schedules.

  The standard format displays a blank period column and an asterisk in the day column for enhanced schedules. Issue FORMAT=DETAILED to display complete information about an enhanced schedule.

Example: Display detailed information on administrative command schedules

From a managed server, display detailed information about administrative command schedules. See Field descriptions for field descriptions.

```
query schedule * type=administrative
format=detailed

                Schedule Name: BACKUP_ARCHIVEPOOL
                  Description:
                      Command: backup db
```

```
                      Priority: 5
                 Start Date/Time: 2004.06.04 16.57.15
                      Duration: 1 Hour(s)
    Maximum Run Time (Minutes): 0
                 Schedule Style: Classic
                        Period: 1 Day(s)
                   Day of Week: Any
                         Month:
                  Day of Month:
                 Week of Month:
                    Expiration:
                        Active: No
Last Update by (administrator): $$CONFIG MANAGER$$
         Last Update Date/Time: 2004.06.04 17.51.49
              Managing Profile: ADMIN_INFO

                  Schedule Name: MONTHLY_BACKUP
                    Description:
                        Command: q status
                      Priority: 5
                 Start Date/Time: 2004.06.04 16.57.14
                      Duration: 1 Hour(s)
    Maximum Run Time (Minutes): 0
                 Schedule Style: Enhanced
                        Period:
                   Day of Week: Tue,Thu,Fri
                         Month: Aug,Nov
                  Day of Month:
                 Week of Month: Second,Third
                    Expiration:
                        Active: No
Last Update by (administrator): $$CONFIG MANAGER
         Last Update Date/Time: 2004.06.04 17.51.49
              Managing Profile: ADMIN_INFO
```

Field descriptions

Schedule Name
: Specifies the name of the schedule.

Description
: Specifies the description of the schedule.

Command
: Specifies the command that is scheduled.

Priority
: Specifies the priority value for this schedule.

Start Date/Time
: Specifies the initial starting date and time for this schedule.

Duration
: Specifies the length of the startup window.

Maximum Run Time (Minutes)
: Specifies the number of minutes during which server processes that are started by the scheduled commands must be completed. If processes are still running after the maximum run time, the central scheduler cancels the processes.
  Tips:

  - This parameter does not apply to some processes, such as duplicate-identification processes, which can continue to run after the maximum run time.
  - Another cancel time might be associated with some commands. For example, the MIGRATE STGPOOL command can include a parameter that specifies the length of time that the storage pool migration runs before the migration is automatically canceled. If you schedule a command for which a cancel time is defined, and you also define a maximum run time for the schedule, the processes are canceled at whichever cancel time is reached first.

Schedule Style
: Specifies whether classic or enhanced schedule rules are used.

Period
: Specifies the time between startup windows (assuming DAYOFWEEK=ANY). This is not displayed for enhanced syntax schedules.

Day of Week

Specifies the day of the week on which the startup windows begin.

Month
: Specifies the months during which the schedule will run. This is not displayed for classic syntax schedules.

Day of Month
: Specifies the days of the month during which the schedule will run. This is not displayed for classic syntax schedules.

Week of Month
: Specifies the weeks (first, second, third, fourth, or last) of the month during which the schedule will run. This is not displayed for classic syntax schedules.

Expiration
: Specifies the date after which this schedule will no longer be used. If this column is blank, the schedule does not expire.

Active?
: Specifies whether the schedule has been processed according to the time and date set for this schedule.

Last Update by (administrator)
: Specifies the name of the administrator that most recently updated the schedule. If this field contains a $$CONFIG_MANAGER$$, the schedule is associated with a domain that is managed by the configuration manager.

Last Update Date/Time
: Specifies the last date and time the schedule was modified.

Managing Profile
: Specifies the profile or profiles to which the managed server subscribed to get the definition of this schedule.

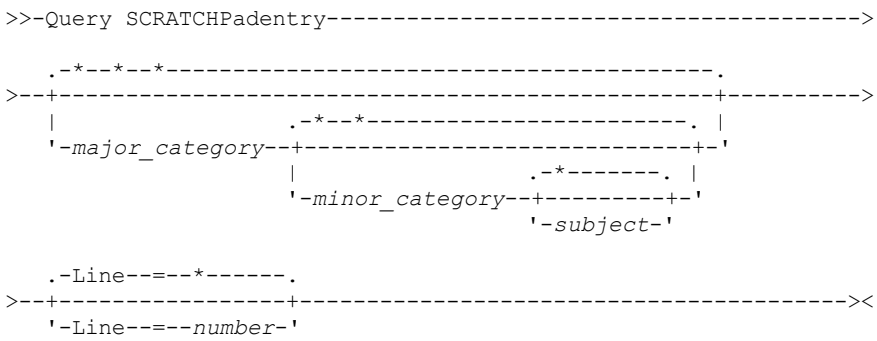
QUERY SCRATCHPADENTRY (Query a scratch pad entry)

Use this command to display data that is contained in the scratch pad.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

major_category
: Specifies the major category to be queried. This parameter is case sensitive. You can query all major categories by omitting this parameter.

minor_category
: Specifies the minor category to be queried. This parameter is case sensitive. You can query all minor categories in the major category by omitting this parameter.

subject
: Specifies the subject to be queried. This parameter is case sensitive. You can query all subjects in the minor category by omitting this parameter.

Line
: Specifies the number of the line to be queried. For *number*, enter an integer in the range 1 - 1000. You can query all lines of data in the subject by omitting this parameter.

Example: Query scratch pad entries

Query a database that stores information about the location of all administrators.

```
query scratchpadentry admin_info location

Scratchpad major category: admin_info
     Scratchpad minor category: location
            Scratchpad subject: codjo
        Scratchpad line number: 1
               Scratchpad data: Toronto 5A24
         Date/time of creation: 2013-09-10, 10:15:50
         Last Update Date/Time: 2013-09-10, 10:15:50
Last Update by (administrator): CODJO

     Scratchpad major category: admin_info
     Scratchpad minor category: location
            Scratchpad subject: jane
        Scratchpad line number: 1
               Scratchpad data: Raleigh GF85
         Date/time of creation: 2013-09-09, 14:29:40
         Last Update Date/Time: 2013-09-09, 14:29:40
Last Update by (administrator): JANE_W

     Scratchpad major category: admin_info
     Scratchpad minor category: location
            Scratchpad subject: jane
        Scratchpad line number: 2
               Scratchpad data: Out of the office from 1-15 Nov.
         Date/time of creation: 2013-09-09, 14:30:05
         Last Update Date/Time: 2013-10-31, 16:55:52
Last Update by (administrator): JANE_W

     Scratchpad major category: admin_info
     Scratchpad minor category: location
            Scratchpad subject: montse
        Scratchpad line number: 1
               Scratchpad data: Barcelona B19
         Date/time of creation: 2013-09-10, 04:34:37
         Last Update Date/Time: 2013-09-10, 04:34:37
Last Update by (administrator): MONTSERRAT
```

Field descriptions

Scratchpad data
: The data that is stored in the scratch pad entry.

Date/time of creation
: The date and time at which the scratch pad entry was created.

Last Update Date/Time
: The date and time at which the scratch pad entry was last updated.

Last Update by (administrator)
: The administrator who last updated the scratch pad entry.

Related commands

Table 1. Commands related to QUERY SCRATCHPADENTRY

Command	Description
DEFINE SCRATCHPADENTRY	Creates a line of data in the scratch pad.
DELETE SCRATCHPADENTRY	Deletes a line of data from the scratch pad.
SET SCRATCHPADRETENTION	Specifies the amount of time for which scratch pad entries are retained.
UPDATE SCRATCHPADENTRY	Updates data on a line in the scratch pad.

QUERY SCRIPT (Query IBM Spectrum Protect scripts)

Use this command to display information about scripts.

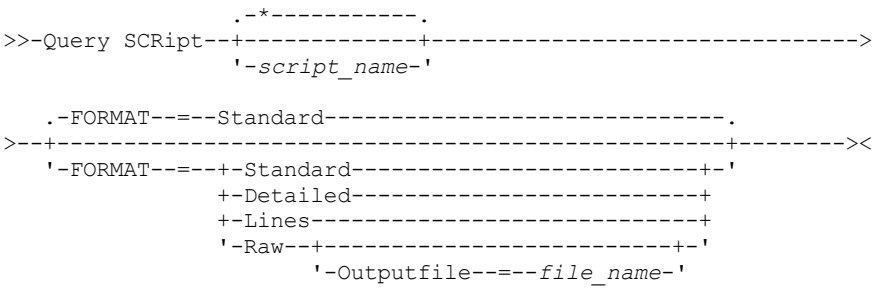
You can use this command with the DEFINE SCRIPT command to create a new script by using the contents from another script.

Privilege class

The privilege class that is required for this command depends on whether the Outputfile parameter is specified in the command.

- If the Outputfile parameter is not specified, any administrator can issue this command.
- If the Outputfile parameter is specified and the REQSYSAUTHOUTFILE server option is set to YES, the administrator must have system privilege.
- If the Outputfile parameter is specified and the REQSYSAUTHOUTFILE server option is set to NO, the administrator must have operator, policy, storage, or system privilege.

Syntax



Parameters

script_name
: Specifies the name of the script for which information is to be displayed. You can include a wildcard character to specify this name.
Important: If you do not specify a script, the query displays information about all scripts. The time that is used to process this command and the amount of information that is displayed can be extensive.

Format
: Specifies the output format for displaying script information. The default is STANDARD. Possible values are:

  Standard
  : Specifies that only the script name and description in a script are displayed.

  Detailed
  : Specifies that detailed information about the script is displayed. This information includes the commands in the script and their line numbers, the date of the last update and the administrator that completed the updates.

  Lines
  : Specifies that the script name, the line number of the commands, comment lines, and the commands in the script are displayed.

  Raw
  : Specifies that commands contained in the script are written to a file named with the Outputfile parameter. This format is a way of directing output from a script to a file so that it can be copied into another script by using the DEFINE SCRIPT command.

    If no output file is specified, the IBM Spectrum Protect™ server outputs the "query script" with "format=raw" to the console.

Outputfile
: Specifies the name of the file to which output is directed when you specify FORMAT=Raw. The file that you specify must be on the server that is running this command. If the file exists, the query output is appended to the end of the file.

Example: List the script descriptions

Display the standard information about scripts.

```
query script *

Name             Description
---------------  --------------------------------------------------
```

```
QCOLS           Display columns for a specified SQL table
QSAMPLE         Sample SQL Query
EXAMPLE         Backup the store pools and database when no sessions
```

Example: Display the contents of a script with line numbers

Display the lines of information for a script named Q_AUTHORITY.

```
query script q_authority format=lines
```

```
Name         Line    Command
             Number
----------   ------  ------------------------------------------------
Q_AUTHORITY  1       /* ----------------------------------------*/
             5       /* Script Name:  Q_AUTHORITY               */
             10      /* Description: Display administrators that  */
             15      /*              have the authority to issue  */
             20      /*              commands requiring a         */
             25      /*              specific privilege.          */
             30      /* Parameter 1: privilege name - in the form */
             35      /*              x_priv - EX. policy_priv     */
             40      /* Example:  run q_authority storage_priv    */
             45      /* ----------------------------------------*/
             50      select admin_name from admins where -
             55        upper(system_priv) <> 'NO' or -
             60        upper($1) <> 'NO'
```

Example: Create a script from an existing script

Query the ENGDEV script and direct the output to a file named MY.SCRIPT.

```
query script engdev format=raw outputfile=my.script
```

Example: Display detailed script information

Display detailed information about scripts. See Field descriptions for field descriptions.

```
query script * format=detailed
```

```
                       Name: QCOLS
                Line Number: DESCRIPTION
                    Command: Display columns for a specified SQL
                             table
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 12/02/1997 16:05:29

                       Name: QCOLS
                Line Number: 1
                    Command: select colname from columns where
                             tabname='$1'
Last Update by (administrator): SERVER_CONSOLE
         Last Update Date/Time: 12/02/1997 16:05:29
```

Field descriptions

Name
: The name of the script.

Line Number
: The line number of the script or the string DESCRIPTION.

Command
: The command included on the line number that is displayed in the previous field.

Last Update by (administrator)
: The name of the administrator that defined or most recently updated the script.

Last Update Date/Time
: The date and time that the administrator defined or updated the script.

Related commands

Table 1. Commands related to QUERY SCRIPT

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

Related concepts:
Server scripts

QUERY SERVER (Query a server)

Use this command to display information about a server definition.

Privilege class

Any administrator can issue this command.

Syntax

```
                .-*-----------.  .-Format--=--Standard-----.
>>-Query SERver--+-------------+--+-------------------------+--><
                '-server_name-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'
```

Parameters

server_name
: Specifies the name of the server to be queried. You can use wildcard characters to specify this name. This parameter is optional. The default is all server names.

Format
: Specifies how the information is displayed. The parameter is optional. The default is STANDARD.

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: List all servers

Display information in standard format about all servers. See Field descriptions for field descriptions.

```
query server *
```

```
Server   Comm.   High-level  Low-level Days  Server   Virtual  Allow
Name     Method  Address     Address   Since Password Volume   Replace-
                                       Last  Set      Password ment
                                       Access         Set
-------- ------ ----------- --------  ------ ------- -------- --------
SERVER_A TCPIP  9.115.35.6  1501         11  Yes      No       No
SERVER_B TCPIP  9.115.45.24 1500         <1  Yes      No       No
ASTRO    TCPIP  9.115.32.21 1500         24  Yes      No       No
```

Example: Display detailed information about a specific server

From a managed server, display detailed information about SERVER_A. See Field descriptions for field descriptions.

```
query server server_a format=detailed


                                Server Name: SERVER_A
                             Comm. Method: TCPIP
                          Transfer Method: TCPIP
                        High-level Address: 9.115.4.15
                         Low-level Address: 1500
                                Description:
                         Allow Replacement: No
                                Node Name:
                     Last Access Date/Time: 07/09/2013 09:00:00
                    Days Since Last Access: <1
                               Compression: Client's choice
                  Archive Delete Allowed?: No
                                      URL:
                     Registration Date/Time: 07/08/2013 09:15:09
                  Registering Administrator: $$CONFIG_MANAGER$$
                Bytes Received Last Session: 362
                    Bytes Sent Last Session: 507
                   Duration of Last Session: 0.00
                 Pct. Idle Wait Last Session: 0.00
                Pct. Comm. Wait Last Session: 0.00
                Pct. Media Wait Last Session: 0.00
                       Grace Deletion Period: 5
                            Managing profile:
                      Server Password Set: Yes
           Server Password Set Date/Time: 07/08/2013 09:15:09
         Days Since Server Password Set: 1
       Invalid Sign-on Count for Server: 0
            Virtual Volume Password Set: No
  Virtual Volume Password Set Date/Time: (?)
 Days Since Virtual Volume Password Set: (?)
Invalid Sign-on Count for Virtual Volume Node: 0
                     Validate Protocol: No
                               Version: 7
                               Release: 1
                                 Level: 0.0
                               Role(s): Replication
                                   SSL: No
                    Session Security: Strict
                    Transport Method: TLS 1.2
```

Field descriptions

Server Name
: The name of the server.

Comm. Method
: The communication method that is used to connect to the server.

Transfer Method
: The method that is used for server-to-server data transfer.

High-level Address
: The IP address (in dotted decimal format) of the server.

Low-level Address
: The port number of the server.

Description
: The server description.

Allow Replacement
: Specifies whether a server definition on a managed server can be replaced with a definition from a configuration manager.

Node Name
: The name of the client node.

Last Access Date/Time
: The last date and time that the client node accessed the server.

Days Since Last Access
: The number of days since the client node accessed the server.

Compression
: The type of compression that is completed by IBM Spectrum Protect™ on client files.

Archive Delete Allowed?

Specifies whether the client node can delete its own archive files. A value of (?) denotes that this field is not set and does not apply to this definition.

URL
The URL used to access this server from a web browser-based interface.

Registration Date/Time
The date and time that the client node was registered.

Registering Administrator
The name of the administrator that registered the client node.

Bytes Received Last Session
The number of bytes received by the server during the last client node session.

Bytes Sent Last Session
The number of bytes sent to the client node.

Duration of Last Session
The length of the last client node session, in seconds.

Pct. Idle Wait Last Session
The percentage of the total session time during which the client did not complete any functions.

Pct. Comm. Wait Last Session
The percentage of the total session time that the client waited for a response from the server.

Pct. Media Wait Last Session
The percentage of the total session time that the client waited for a removable volume to be mounted.

Grace Deletion Period
The number of days an object remains on the target server after it is marked for deletion.

Managing Profile
The profile from which the managed server got the definition of this server.

Server Password Set
Specifies whether the password for the server is set.

Server Password Set Date/Time
Specifies when the password for the server is set.

Days since Server Password Set
The number of days since the server password was set.

Invalid Sign-on count for Server
The maximum number of invalid sign-on attempts that the server can accept.

Virtual Volume Password Set
Specifies whether the password used to log on to the target server is set.

Virtual Volume Password Set Date/Time
Specifies when the password for virtual volume support is set.

Days Since Virtual Volume Password Set
The number of days since the password for virtual volume support was set.

Invalid Sign-on Count for Virtual Volume Node
The maximum number of invalid sign-on attempts that are accepted on the target server.

Validate Protocol (deprecated)

Specifies whether the storage agent has the data validation function enabled. This field is deprecated.

Version
The software version of the IBM Spectrum Protect server.

Release
The software release of the IBM Spectrum Protect server.

Level
The software level of the IBM Spectrum Protect server.

Role(s)
The role of the server. For example, one of the roles that the server is used for is replication.

SSL
Specifies whether Secure Sockets Layer (SSL) communication is used.

Session Security
Specifies the level of session security that is enforced for the server. Values can be STRICT or TRANSITIONAL.

Transport Method
Specifies the transport method that was last used for the specified server. Values can be TLS 1.2, TLS 1.1, or NONE. A question mark (?) is displayed until a successful authentication is completed.

Related commands

Table 1. Commands related to QUERY SERVER

Command	Description
DEFINE DEVCLASS	Defines a device class.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE DEVCLASS	Deletes a device class.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
DELETE SERVER	Deletes the definition of a server.
AIX Linux Windows PROTECT STGPOOL	AIX Linux Windows Protects a directory-container storage pool.
QUERY NODE	Displays partial or complete information about one or more clients.
RECONCILE VOLUMES	Reconciles source server virtual volume definitions and target server archive objects.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET REPLSERVER	Specifies a target replication server.
UPDATE DEVCLASS	Changes the attributes of a device class.
UPDATE NODE	Changes the attributes that are associated with a client node.
UPDATE SERVER	Updates information about a server.

QUERY SERVERGROUP (Query a server group)

Use this command to display information about server groups and group members.

Privilege class

Any administrator can issue this command.

Syntax

```
                      .-*----------.
>>-QUERY SERVERGroup--+------------+--------------------------><
                      '-group_name-'
```

Parameters

group_name
Specifies the server group to query. This parameter is optional. You can use wildcard characters to specify this name.

Example: List server groups

From a managed server, query all server groups. Field descriptions for field descriptions.

```
query servergroup *

Server Group    Members         Description          Managing Profile
------------    ------------    -----------------    ----------------
```

```
ADMIN_GROUP     SERVER_A        Headquarters         ADMIN_INFO
                SERVER_B
                SERVER_C
                SERVER_D
```

Field descriptions

Server Group
: The name of the server group.

Members
: The group members.

Description
: The description of the server group.

Managing Profile
: The profile or profiles to which the managed server subscribed to get the definition of the server groups.

Related commands

Table 1. Commands related to QUERY SERVERGROUP

Command	Description
COPY SERVERGROUP	Creates a copy of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE SERVERGROUP	Deletes a server group.
QUERY SERVER	Displays information about servers.
RENAME SERVERGROUP	Renames a server group.
UPDATE SERVERGROUP	Updates a server group.

QUERY SESSION (Query client sessions)

Use this command to display information about administrative, node, and server sessions.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query SEssion--+---------+-----------------------------------><
                  '-sessnum-'

>--+-----------------------------+-----------------------------><
   '-MINTIMethreshold--=--minutes-'

>--+---------------------------------------+-------------------><
   '-MAXTHRoughput--=--kilobytes_per_second-'

   .-Format--=--Standard-----.  .-Type--=--*----------.
>--+-------------------------+--+--------------------+---------><
   '-Format--=--+-Standard-+-'  '-Type--=--+-Admin--+-'
                '-Detailed-'               +-Node---+
                                           '-Server-'

   .-CLIENTName--=--*---------------.
>--+-------------------------------+--------------------------><
   '-CLIENTName--=----client_name---'
```

Parameters

sessnum

Specifies the number of the administrative or client node session to query. This parameter is optional. If you do not specify a value for this parameter, all sessions display.

MINTIMethreshold
Specifies to display sessions that had at least this number of minutes elapse from the time the client sent data to the server for storage. This parameter is optional. The minimum number of minutes is 1. The maximum number of minutes is 99999999.

MAXTHRoughput
Specifies to display sessions that are transferring data at a rate less than this number of kilobytes per second. This parameter is optional. The minimum number of kilobytes per second is 0. The maximum number of kilobytes per second is 99999999.

Format
Specifies how the information displays. This parameter is optional. The default value is STANDARD. The following values are possible:

Standard
Specifies that partial information displays for the session.

Detailed
Specifies that complete information displays for the session.

Type
Specifies the type of sessions to include in the query results. If you do not specify a value for this parameter, all types of sessions are queried. This parameter is optional. You can specify one of the following values:

Admin
Specifies that administrative sessions are displayed.

Node
Specifies that node sessions are displayed.

Server
Specifies that server sessions are displayed.

CLIENTName
Specifies the name of an administrator, client node, or server to be queried. You can specify one or more names. You can also specify node groups and proxy nodes. If you specify multiple names, separate the names with commas; use no intervening spaces. You can use wildcard characters with node names but not with node group names. The parameter is optional.

During node replication, the client name on the target server is displayed as *node_name (server_name)*, where *node_name* is the node whose data is being replicated, and *server_name* is the name of the source server. You can specify either the node name or the server name in the CLIENTName parameter to display the replication sessions.

Example: List active client node sessions

Display information about all administrative and client node sessions that are communicating with the server. See Field descriptions for field descriptions.

```
query session
```

```
  Sess Comm.  Sess     Wait   Bytes   Bytes Sess  Platform Client
Number Method State    Time    Sent   Recvd Type           Name
------ ------ ------ ------ ------- ------- ----- -------- ------
     4  TCP/IP  Run    0 S    1.4 K    162   Admin  WinNT   ADMIN
```

Example: Display detailed information about active client node sessions

Display detailed information about all administrative and client node sessions that are communicating with the server. See Field descriptions for field descriptions.

```
query session format=detailed
```

```
             Sess Number: 4
            Comm. Method: Tcp/Ip
              Sess State: Run
               Wait Time: 0 S
              Bytes Sent: 1.4 K
             Bytes Recvd: 162
               Sess Type: Admin
```

```
                Platform: WinNT
             Client Name: ADMIN
      Media Access Status:
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:
                 Actions:
           Failover Mode: No
```

Field descriptions

Sess Number
: Specifies a unique session identification number that is assigned by the server.

Comm. Method
: Specifies the method that is used by the client to communicate with the server.

Sess State
: Specifies the current communications state of the server. The following states are possible:

  End
  : The session is ending (session resources are released).

  IdleW
  : Waiting for client's next request (session is idle).

  MediaW
  : The session is waiting for access to a sequential access volume.

  RecvW
  : Waiting to receive an expected message from the client.

  Run
  : The server is running a client request (and not waiting to send data).

  SendW
  : The server is waiting to send data to the client (waiting for data to be delivered to the client node that was already sent).

  SSLiW
  : The session is waiting for Secure Sockets Layer (SSL) initialization to complete.

  Start
  : The session is starting (authentication is in progress).

Wait Time
: Specifies the amount of time (seconds, minutes, or hours) the server is in the current state shown.

Bytes Sent
: Specifies the number of bytes of data that is sent to the client node since the session was initiated.

Bytes Recvd
: Specifies the number of bytes of data that is received from the client node since the session was initiated.

Sess Type
: Specifies the type of session in process: ADMIN for an administrative session, NODE for a client node session, or SERVER. SERVER specifies the server starts a session and initiates server-to-server operations such as central configuration, library sharing, and storage agent sessions.

Platform
: Specifies the type of operating system that is associated with the client.

Client Name
: Specifies the name of the client node or the administrator.

  For node replication sessions, the client name is updated to *node_name (server_name)* on the target server after data transfer starts.

Media Access Status
: Specifies the type of media wait state. When a session is in a media wait state, this field displays a list of all mount points and sequential volumes for the session. The list of mount points specifies the device class and the associated storage pool. The list of volumes specifies the primary storage pool volumes in addition to any copy storage pool and active-data pool volumes along with their assigned storage pool.

  The server allows multiple sessions to read and one session to write to a volume concurrently in a storage pool that is associated with the FILE or CENTERA device type. As a result, a volume in a storage pool with a device type of FILE or CENTERA can appear as the current volume for more than one session.

Proxy by Storage Agent

Specifies the storage agent that is the proxy for LAN-free data movement for the node.

User Name
: Specifies the user ID of the node, on a multi-user system, that connects to the server when it is not the same system user who originally connected to the server.

Date/Time First Data Sent
: Specifies the date and time that the client first sent data to the server for storage.

Actions
: Displays a list of actions that are performed during the session. An action is listed only once, even if the action occurs multiple times during a session. The following actions are possible:

  BkIns
  : One or more backup objects were stored on the server. The operation might have been an incremental backup or a selective backup.

  BkUpd
  : One or more attributes were updated for a backup object that is stored on the server.

  BkDel
  : One or more backup objects that are stored on the server are deleted.

  BkRebind
  : One or more backup objects that are stored on the server are bound to a different management class.

  NoQueryRestore
  : A no-query restore operation was initiated from the client to restore backed-up files from the server to the client system.

  ArIns
  : One or more archive objects were stored on the server.

  ObjRtrv
  : One or more files were retrieved from the server. This might have been to retrieve archive files, or to restore backup data (except for backup data from a no-query restore operation).

  MigIns
  : One or more files are migrated and stored on the server by IBM Spectrum Protect™ for Space Management (HSM client).

  MigDel
  : One or more space-managed files that were stored on the server are deleted.

  MigRebind
  : One or more space-managed files that are stored on the server are bound to a different management class.

  MigRecall
  : One or more space-managed files that are stored on the server are recalled.

  MigUpd
  : The attributes for one or more space-managed files that are stored on the server are updated.

  FSAdd
  : The client node added one or more new file spaces to server storage.

  FSUpd
  : The client node updated attributes for one or more file spaces that are defined to the server.

  DefAuth
  : A SET ACCESS command is processed by the client node, which caused an authorization rule for access to the client node's data to be added.

Failover Mode
: Specifies whether the client session was started in failover mode. The following values are possible:

  Force
  : The FORCEFAILOVER flag is specified on the client and the session is forced into failover mode.

  Yes
  : The client session was started in failover mode.

  No
  : The client session was not started in failover mode.

Related commands

Table 1. Command related to QUERY SESSION

Command	Description
CANCEL SESSION	Cancels active sessions with the server.

QUERY SHREDSTATUS (Query shredding status)

Use this command to display information about data waiting to be shredded.

Privilege class

To issue this command you must have administrator privilege.

Syntax

```
                        .-Format--=--Standard-----.
>>-QUERY SHREDstatus--+-------------------------+-------------><
                      '-Format--=--+-Standard-+-'
                                   '-Detailed-'
```

Parameters

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed. This is the default.

  Detailed
  : Specifies that complete information is displayed.

Example: Display summary shredding information

Show partial information about data shredding on the server. See Field descriptions for field descriptions.

```
query shredstatus

Shredding      Objects
  Active      Awaiting
                 Shred
 -------      --------
      NO             4
```

Example: Display detailed shredding information

Display detailed information about data shredding on the server. See Field descriptions for field descriptions.

```
query shredstatus format=detailed

Shredding  Objects  Occupied   Data Left
  Active   Awaiting   Space    To Shred
            Shred     (MB)        (MB)
--------- --------  --------  ----------
    NO         4        182         364
```

Field descriptions

Shredding Active
: Indicates whether or not the server is actively shredding data at this time.

Objects Awaiting Shred
: The number of objects currently waiting to be shredded.

Occupied Space (MB)
: The amount of server storage space occupied by the objects currently waiting to be shredded, in megabytes. This is the amount of space that will become available when the objects are shredded.

Data Left to Shred (MB)
: The amount of data that still needs to be shredded.

Related commands

Table 1. Commands related to QUERY SHREDSTATUS

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
EXPORT NODE	Copies client node information to external media or directly to another server.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
MOVE DATA	Moves data from a specified storage pool volume to another storage pool volume.
QUERY STGPOOL	Displays information about storage pools.
SETOPT	Updates a server option without stopping and restarting the server.
SHRED DATA	Manually starts the process of shredding deleted data.
UPDATE STGPOOL	Changes the attributes of a storage pool.

QUERY SPACETRIGGER (Query the space triggers)

Use this command to display the settings for storage pool space triggers.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query SPACETrigger--STG--+-------------------------+-------->
                            '-STGPOOL--=--storage_pool-'

   .-Format--=--Standard-----.
>--+-------------------------+-------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

STG
: Specifies a storage pool space trigger.

STGPOOL
: Specifies one or more storage pools (using a wildcard) for which storage pool trigger information will be displayed. If STG is specified but STGPOOL is not, the default storage pool space trigger, if any, is displayed.

Format
: Specifies how the information is displayed. This parameter is optional. The default is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display detailed settings for a storage pool space trigger

Issue this command:

```
query spacetrigger stg stgpool=archivepool format=detailed
```

AIX

```
         STGPOOL Full Percentage:   50
   STGPOOL Expansion Percentage:    20
       STGPOOL Expansion prefix:    /usr/tivoli/tsm/server/filevol/
                        STGPOOL:    ARCHIVEPOOL
 Last Update by (administrator):    SERVER_CONSOLE
          Last Update Date/Time:    05/10/2004 11:59:59
```

Linux

```
         STGPOOL Full Percentage:   50
   STGPOOL Expansion Percentage:    20
       STGPOOL Expansion prefix:    /opt/tivoli/tsm/server/filevol/
                        STGPOOL:    ARCHIVEPOOL
 Last Update by (administrator):    SERVER_CONSOLE
          Last Update Date/Time:    05/10/2004 11:59:59
```

Windows

```
         STGPOOL Full Percentage:   50
   STGPOOL Expansion Percentage:    20
       STGPOOL Expansion prefix:    c:\program files\tivoli\filevol\
                        STGPOOL:    ARCHIVEPOOL
 Last Update by (administrator):    SERVER_CONSOLE
          Last Update Date/Time:    05/10/2004 11:59:59
```

Field descriptions

STGPOOL Full Percentage
: The trigger utilization percentage at which IBM Spectrum Protect™ allocates more space for the storage pool.

STGPOOL Expansion Percentage
: The percentage of space by which the storage pool should be expanded.

STGPOOL Expansion prefix
: The prefix associated with the space trigger.

STGPOOL
: The storage pool name associated with the query.

Last Update by (administrator)
: The administrator who last updated the storage pool space trigger.

Last Update Date/Time
: The date and time when the administrator last updated the storage pool space trigger.

Related commands

Table 1. Commands related to QUERY SPACETRIGGER

Command	Description
DEFINE SPACETRIGGER	Defines a space trigger to expand the space for a storage pool.
DELETE SPACETRIGGER	Deletes the storage pool space trigger.
UPDATE SPACETRIGGER	Changes attributes of storage pool space trigger.

QUERY STATUS (Query system parameters)

Use the QUERY STATUS command to display information about system parameters.

Use this command for the following reasons:

- To display the service level of the server
- To display information about the general server parameters, such as those defined by the SET commands
- To request information about client sessions, such as the availability of the server, password authentication, accounting settings, or the retention period for the information that is retained in the activity log
- To display information about the central scheduler, such as the central scheduling mode of the server
- To display the maximum number of repeated attempts that are allowed after a failed attempt to run a scheduled command
- To display whether subfiles can be backed up to this server, as indicated by the SET SUBFILE command
- To display information about a target replication server

- To display licensing information

Tip: To display information about a target replication server, you must issue the command from the target replication server.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query STatus-------------------------------------------------><
```

Parameters

None.

Example: Query the status of a configuration manager

Display general information about server parameters. The command is run from a configuration manager. For descriptions of displayed fields, see Field descriptions.

```
query status
```

AIX

```
                         Server Name: SETSHOT
      Server host name or IP address: setshot
           Server TCP/IP port number: 1500
                         Crossdefine: On
                  Server Password Set: Yes
       Server Installation Date/Time: 2016-07-08,   09:45:53
            Server Restart Date/Time: 2016-10-10,   05:38:49
                      Authentication: Off
         Password Expiration Period: 9,999 Day(s)
       Invalid Sign-on Attempt Limit: 0
             Minimum Password Length: 8
                        Registration: Closed
                     Subfile Backup: Client
                       Availability: Enabled
          Inbound Sessions Disabled:
         Outbound Sessions Disabled:
                          Accounting: Off
            Activity Log Retention: 30 Day(s)
      Activity Log Number of Records: 222919
                  Activity Log Size: 6 M
  Activity Summary Retention Period: 30 Day(s)
               License Audit Period: 30 Day(s)
                 Last License Audit: 2016-10-21,   07:40:20
          Server License Compliance: Valid
                  Central Scheduler: Active
                   Maximum Sessions: 300
         Maximum Scheduled Sessions: 75
      Event Record Retention Period: 14 Day(s)
             Client Action Duration: 5 Day(s)
  Schedule Randomization Percentage: 25
               Query Schedule Period: Client
            Maximum Command Retries: Client
                        Retry Period: Client
Client-side Deduplication Verification Level: 0 %
                     Scheduling Modes: Any
                     Active Receivers: CONSOLE ACTLOG
            Configuration manager?: Off
                     Refresh interval: 60
            Last refresh date/time:
                     Context Messaging: On
Table of Contents (TOC) Load Retention: 120 Minute(s)
          Machine Globally Unique ID: d4.cg.f6.ae.04.6e.11.e3.80.1f.00.21.5e.18.df.01
       Archive Retention Protection: Off
              Database Directories: /TSMserver/DB1,/TSMserver/DB2
```

```
              Total Space of File System (MB): 222,720.00
               Used Space on File System (MB): 47,780.74
                   Free Space Available (MB): 174,939.26
                         Encryption Strength: AES
     Client CPU Information Refresh Interval: 180
                       Outbound Replication: Enabled
                  Target Replication Server: POWER
        Default Replication Rule for Archive: ALL_DATA
         Default Replication Rule for Backup: ALL_DATA
Default Replication Rule for Space Management: ALL_DATA
         Replication Record Retention Period: 30 Day(s)
                                   LDAP User:
                          LDAP Password Set: No
                     Default Authentication: Local
                 Failover High Level Address:
                       Scratchpad retention: 365 Day(s)
       Replication Recovery of Damaged Files: On
                          SUR Occupancy (TB): 5.66
                   SUR Occupancy Date/Time: 2016-10-10,   05:39:33
                   Front-End Capacity (MB): 226,331
                    Front-End Client Count: 6
                   Front-End Capacity Date: 2016-10-13, 09:20:02
                          Product Offering: IBM Spectrum Protect
```

Linux

```
                               Server Name: GOBI
            Server host name or IP address:
                 Server TCP/IP port number: 1500
                               Crossdefine: On
                       Server Password Set: Yes
             Server Installation Date/Time: 2016-07-08,   11:29:03
                  Server Restart Date/Time: 2016-11-10,   14:25:03
                             Authentication: On
               Password Expiration Period: 90 Day(s)
             Invalid Sign-on Attempt Limit: 0
                   Minimum Password Length: 8
                                Registration: Closed
                              Subfile Backup: No
                                Availability: Enabled
                Inbound Sessions Disabled:
               Outbound Sessions Disabled:
                                  Accounting: Off
                 Activity Log Retention: 30 Day(s)
            Activity Log Number of Records: 21346
                           Activity Log Size: <1 M
        Activity Summary Retention Period: 30 Day(s)
                        License Audit Period: 30 Day(s)
                          Last License Audit: 2016-10-21,   23:27:23
                Server License Compliance: Valid
                         Central Scheduler: Active
                          Maximum Sessions: 500
               Maximum Scheduled Sessions: 250
            Event Record Retention Period: 14 Day(s)
                    Client Action Duration: 5 Day(s)
        Schedule Randomization Percentage: 25
                     Query Schedule Period: Client
                Maximum Command Retries: Client
                             Retry Period: Client
 Client-side Deduplication Verification Level: 0 %
                          Scheduling Modes: Any
                          Active Receivers: CONSOLE ACTLOG
                Configuration manager?: Off
                          Refresh interval: 60
                Last refresh date/time:
                          Context Messaging: Off
      Table of Contents (TOC) Load Retention: 120 Minute(s)
                Machine Globally Unique ID: fc.e7.be.58.4a.a7.11.e0.8a.c8.e4.1f.13.34.11.e0
             Archive Retention Protection: Off
                      Database Directories:
/TSMdbspace1/gpcinst1,/TSMdbspace2/gpcinst1,/TSMdbspace3/gpcinst1
              Total Space of File System (MB): 302,379.84
               Used Space on File System (MB): 106,793.65
                   Free Space Available (MB): 195,586.20
                         Encryption Strength: AES
```

```
      Client CPU Information Refresh Interval: 180
                          Outbound Replication: Enabled
                      Target Replication Server:
         Default Replication Rule for Archive: ALL_DATA
          Default Replication Rule for Backup: ALL_DATA
Default Replication Rule for Space Management: ALL_DATA
          Replication Record Retention Period: 30 Day(s)
                                    LDAP User:
                               LDAP Password Set: No
                         Default Authentication: Local
                    Failover High Level Address:
                           Scratchpad retention: 365 Day(s)
        Replication Recovery of Damaged Files: Off
                             SUR Occupancy (TB): 0.00
                      SUR Occupancy Date/Time: 2016-10-10,   14:25:35
                      Front-End Capacity (MB): 226,331
                       Front-End Client Count: 6
                      Front-End Capacity Date: 2016-10-13, 09:20:02
                             Product Offering: IBM Spectrum Protect
```

Windows

```
                                  Server Name: EXCELSIOR
                Server host name or IP address: excelsior.storage.
                                                newyork.example.com
                     Server TCP/IP port number: 1500
                                   Crossdefine: On
                               Server Password Set: Yes
                 Server Installation Date/Time: 2016-07-08, 18:02:50
                      Server Restart Date/Time: 2016-11-10, 11:48:32
                                Authentication: On
                   Password Expiration Period: 90 Day(s)
                 Invalid Sign-on Attempt Limit: 0
                       Minimum Password Length: 8
                                  Registration: Closed
                                Subfile Backup: No
                                  Availability: Enabled
                     Inbound Sessions Disabled:
                    Outbound Sessions Disabled:
                                    Accounting: On
                        Activity Log Retention: 30 Day(s)
                Activity Log Number of Records: 1346376
                             Activity Log Size: 37 M
            Activity Summary Retention Period: 30 Day(s)
                          License Audit Period: 30 Day(s)
                            Last License Audit: 2016-10-21, 17:05:16
                    Server License Compliance: Valid
                             Central Scheduler: Active
                              Maximum Sessions: 25
                   Maximum Scheduled Sessions: 12
                 Event Record Retention Period: 14 Day(s)
                        Client Action Duration: 5 Day(s)
              Schedule Randomization Percentage: 25
                          Query Schedule Period: Client
                     Maximum Command Retries: Client
                                  Retry Period: Client
 Client-side Deduplication Verification Level: 0 %
                               Scheduling Modes: Any
                               Active Receivers: CONSOLE ACTLOG
                                                 NTEVENTLOG
                          Configuration manager?: Off
                                Refresh interval: 60
                          Last refresh date/time:
                               Context Messaging: Off
       Table of Contents (TOC) Load Retention: 120 Minute(s)
                    Machine Globally Unique ID: e9.3e.f1.70.ff.c5.11.e2.
                                                a5.67.5c.f3.fc.0c.5e.60
                  Archive Retention Protection: Off
                           Database Directories: e:\Server1\TSMDBdir
                Total Space of File System (MB): 102,270.00
                 Used Space on File System (MB): 22,032.79
                     Free Space Available (MB): 80,237.20
                             Encryption Strength: AES
      Client CPU Information Refresh Interval: 180
```

```
                        Outbound Replication: Enabled
                   Target Replication Server: EXPLORER
         Default Replication Rule for Archive: ALL_DATA
          Default Replication Rule for Backup: ALL_DATA
Default Replication Rule for Space Management: ALL_DATA
          Replication Record Retention Period: 30 Day(s)
                                    LDAP User: cn=excelsior_ldapadmin,ou=excelsior,
                                               ou=John Doe,dc=tsmadldap,dc=storage,
                                               dc=newyork, dc=example,dc=com
                              LDAP Password Set: Yes
                         Default Authentication: LDAP
                  Failover High Level Address:
                         Scratchpad retention: 365 Day(s)
        Replication Recovery of Damaged Files: On
                           SUR Occupancy (TB): 8.98
                  SUR Occupancy Date/Time: 2016-10-10, 11:49:27
                  Front-End Capacity (MB): 226,331
                   Front-End Client Count: 6
```

Windows

```
                  Front-End Capacity Date: 2016-10-13, 09:20:02
                         Product Offering: IBM Spectrum Protect
```

Field descriptions

Server Name
: Specifies the name of the server.

Server host name or IP address
: Specifies the server TCP/IP address.

Server TCP/IP port number
: Specifies the server port address.

Crossdefine
: Specifies whether another server that is running the DEFINE SERVER command automatically defines itself to this server. See the SET CROSSDEFINE command.

Server Password Set
: Specifies whether the password was set for the server.

Server Installation Date/Time
: Specifies the date and time when the server was installed.

Server Restart Date/Time
: Specifies the last date and time when the server was started.

Authentication
: Specifies whether password authentication is set on or off.

Password Expiration Period
: Specifies the period, in days, after which the administrator or client node password expires.

Invalid Sign-on Attempt Limit
: Specifies the number of invalid sign-on attempts before a node is locked.

Minimum Password Length
: Specifies the minimum number of characters for the password. This value does not apply to configurations where an LDAP server is used.

Registration
: Specifies whether client node registration is open or closed.

Subfile Backup
: Specifies whether subfiles can be backed up to this server, as indicated by the SET SUBFILE command.

Availability
: Specifies whether the server is enabled or disabled.

Inbound Sessions Disabled
: Specifies the names of servers from which server-to-server communications are not allowed. To enable inbound server sessions, use the ENABLE SESSIONS command.

Outbound Sessions Disabled
: Specifies the names of servers to which server-to-server communications are not allowed. To enable outbound server sessions, use the ENABLE SESSIONS command.

Accounting
: Specifies whether an accounting record is generated at the end of each client node session.

Activity Log Retention
: Specifies the number of days information is retained in the activity log, or the size of the log.

Activity Log Number of Records
: Specifies the number of records in the activity log.

Activity Log Size
: Specifies the size of the activity log.

Activity Summary Retention Period
: Specifies the number of days information is retained in the SQL activity summary table.

License Audit Period
: Specifies the period, in days, after which the license manager automatically audits the IBM Spectrum Protect™ license. Additional licensing information is available by using the QUERY LICENSE command.

Last License Audit
: Specifies the date and time when the last license audit occurred. Additional licensing information is available by using the QUERY LICENSE command.

Server License Compliance
: Specifies whether the server is in compliance (Valid) or out of compliance (Failed) with the license terms. Use the QUERY LICENSE command to see what factors are causing the server to fail to comply with the license terms.

Central Scheduler
: Specifies whether central scheduling is running (active or inactive).

Maximum Sessions
: Specifies the maximum number of client/server sessions.

Maximum Scheduled Sessions
: Specifies the maximum number of client/server sessions available for processing scheduled work.

Event Record Retention Period
: Specifies the number of days central scheduler event records are retained.

Client Action Duration
: Specifies the duration of the period during which the client processes the schedule that is defined with the DEFINE CLIENTACTION command.

Schedule Randomization Percentage
: Specifies how much of the startup window is used for running scheduled events in client-polling mode.

Query Schedule Period
: Specifies the frequency with which clients poll the server to obtain scheduled work, in client-polling mode. If the value in this field is Client, the polling frequency is determined by the client node.

Maximum Command Retries
: Specifies the maximum number of times that a client scheduler tries to run a scheduled command after a failed attempt. If the value in this field is Client, the client node determines the maximum number.

Retry Period
: Specifies the number of minutes between failed attempts by the client scheduler to contact the server or to run a scheduled command. If the value in this field is Client, the client node determines the number of minutes.

Client-side Deduplication Verification Level
: Specifies a percentage of extents to be verified by the IBM Spectrum Protect server. The extents are created during client-side data deduplication.

Scheduling Modes
: Specifies the central scheduling modes that are supported by the server.

Active Receivers
: Specifies the receivers for which event logging began.

Configuration manager?
: Specifies whether the server is a configuration manager.

Refresh interval
: Specifies the interval that elapses before the managed server requests a refresh of any changes from a configuration manager.

Last refresh date/time
: If the server is a managed server, specifies the date and time of the last successful refresh of configuration information from the configuration manager.

Context Messaging
: Specifies whether context messaging is enabled or disabled.

Table of Contents (TOC) Load Retention
: Specifies the approximate number of minutes that unreferenced TOC data is retained in the database.

Machine Globally Unique ID
: The globally unique identifier (GUID) as of the last time that the server was started. This GUID identifies the host system to which the current server belongs.

Archive Retention Protection
: Specifies whether archive data retention protection is activated or deactivated.

Database Directories

Specifies the locations of the database directories.

Total Space of File System (MB)
Specifies the total size of the file system.

Used Space on File System (MB)
Specifies the amount of space that is in use on the file system.

Free Space Available (MB)
Specifies the amount of space that is available.

Encryption Strength
Indicates data encryption strength: AES or DES.

Client CPU Information Refresh Interval
Specifies the number of days that elapse between client scans for CPU information that is used for PVU estimation.

Outbound Replication
Specifies whether replication processing is enabled or disabled. If outbound replication is disabled, new replication processes cannot start on the server.

Target Replication Server
Specifies the name of the server that is the target for node replication operations. If a target replication server does not exist, this field is blank.

Default Replication Rule for Archive
Specifies the server replication rule that applies to archive data. The following values are possible:

ALL_DATA
Replicates archive data. The data is replicated with a normal priority.

ALL_DATA_HIGH_PRIORITY
Replicates archive data. The data is replicated with a high priority.

NONE
Archive data is not replicated.

Default Replication Rule for Backup
Specifies the server replication rule that applies to backup data. The following values are possible:

ALL_DATA
Replicates active and inactive backup data. The data is replicated with a normal priority.

ACTIVE_DATA
Replicates only active backup data. The data is replicated with a normal priority.
Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

- When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
- When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
- When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
Replicates active and inactive backup data. The data is replicated with a high priority.

ACTIVE_DATA_HIGH_PRIORITY

This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

NONE
Backup data is not replicated.

Default Replication Rule for Space Management
Specifies the server replication rule that applies to space-managed data. The following values are possible:

ALL_DATA
Replicates space-managed data. The data is replicated with a normal priority.

ALL_DATA_HIGH_PRIORITY
Replicates space-managed data. The data is replicated with a high priority.

NONE
Space-managed data is not replicated.

Replication Record Retention Period

Specifies the number of days that replication history records are retained in the database of the source replication server.

LDAP User

Specifies the user ID that is named in the SET LDAPUSER command. This user ID can issue administrative commands on the namespace that is reserved for IBM Spectrum Protect on the LDAP directory server.

LDAP Password Set

This output field shows if a password is defined for the user ID that is named in the SET LDAPUSER command. The values are YES and NO. If YES, the user ID that is named in the SET LDAPUSER command can issue administrative commands on the LDAP namespace that is reserved for IBM Spectrum Protect. If NO, issue the SET LDAPPASSWORD command to set the password for the user ID that is named in the SET LDAPUSER command.

Default Authentication

Specifies the default password authentication method: LOCAL or LDAP.

Authentication Target	**Authentication Method**
IBM Spectrum Protect server	LOCAL
LDAP directory server	LDAP

When you issue the SET DEFAULTAUTHENTICATION command, you define the resulting authentication method for all REGISTER ADMIN and REGISTER NODE commands. The default is LOCAL.

Failover High Level Address

Specifies the high-level address for the failover server that is used by the client. Client restore operations fail over to this high-level address when the interface that is used by the client is different from the interface that is used by replication.

Scratchpad retention

Specifies the number of days for which scratch pad entries are retained since they were last updated.

Replication Recovery of Damaged Files

Specifies whether node replication is enabled to recover damaged files from a target replication server. This is a system-side setting. If ON is specified, the node replication process can be configured to detect damaged files on a source replication server and replace them with undamaged files from a target replication server. If OFF is specified, damaged files are not recovered from a target replication server.

SUR Occupancy (TB)

If you have an IBM Spectrum Protect Suite (SUR) license, this field specifies the SUR occupancy on the server. The *SUR occupancy* is the amount of space that is used to store data that is managed by the IBM Spectrum Protect products that are included in the SUR bundle.

SUR Occupancy Date/Time

Specifies the date and time when SUR occupancy data was last collected.

Front-End Capacity (MB)

Specifies the amount of primary data that is reported as being backed up by clients. Clients include applications, virtual machines, and systems. This value is used for the front-end licensing model.

Front-End Client Count

Specifies the number of clients that reported capacity usage based on the front-end licensing model.

Front-End Capacity Date

Specifies the date and time when front-end capacity data was last collected.

Product Offering

Specifies a product offering.

Value specified by the SET PRODUCTOFFERING command	**Value shown in the QUERY STATUS command output**
ENTry	IBM Spectrum Protect Entry
DATARet	IBM Spectrum Protect for Data Retention
BASIC	IBM Spectrum Protect
EE	IBM Spectrum Protect Extended Edition
SUIte	IBM Spectrum Protect Suite
SUITECloud	IBM Spectrum Protect Suite - IBM Cloud Object Storage Option
SUITEEntry	IBM Spectrum Protect Suite Entry
SUITEArchive	IBM Spectrum Protect Suite - Archive
SUITEProtectier	IBM Spectrum Protect Suite - ProtecTier
SUITEFrontend	IBM Spectrum Protect Suite - FrontEnd

Value specified by the SET PRODUCTOFFERING command	Value shown in the QUERY STATUS command output
SUITEENTRYFrontend	IBM Spectrum Protect Suite Entry - FrontEnd
CLEAR	NULL

Related commands

Table 1. Commands related to QUERY STATUS

Command	Description
BEGIN EVENTLOGGING	Starts event logging to a specified receiver.
DISABLE REPLICATION	Prevents outbound replication processing on a server.
DISABLE SESSIONS	Prevents new sessions from accessing IBM Spectrum Protect but permits existing sessions to continue.
ENABLE REPLICATION	Allows outbound replication processing on a server.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
END EVENTLOGGING	Ends event logging to a specified receiver.
QUERY LICENSE	Displays information about licenses and audits.
SET ACCOUNTING	Specifies whether accounting records are created at the end of each client session.
SET ACTLOGRETENTION	Specifies the number of days to retain log records in the activity log.
SET CONTEXTMESSAGING	Specifies to turn on context messaging to debug an ANR9999D message.
SET CPUINFOREFRESH	Specifies the number of days between client scans for workstation information used for PVU estimates.
SET CROSSDEFINE	Specifies whether to cross define servers.
SET DEDUPVERIFICATIONLEVEL	Specifies the percentage of extents verified by the server during client-side deduplication.
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET EVENTRETENTION	Specifies the number of days to retain records for scheduled operations.
SET LDAPPASSWORD	Sets the password for the LDAPUSER.
SET LDAPUSER	Sets the user who oversees the passwords and administrators on the LDAP directory server.
SET MAXCMDRETRIES	Specifies the maximum number of retries after a failed attempt to execute a scheduled command.
SET MAXSCHEDSESSIONS	Specifies the maximum number of client/server sessions available for processing scheduled work.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
SET PRODUCTOFFERING	Set the product offering licensed to your enterprise.
SET QUERYSCHEDPERIOD	Specifies the frequency for clients to obtain scheduled work, in client-polling mode.
SET RANDOMIZE	Specifies the randomization of start times within a window for schedules in client-polling mode.

Command	Description
SET REPLRECOVERDAMAGED	Specifies whether node replication is enabled to recover damaged files from a target replication server.
SET RETRYPERIOD	Specifies the time between retry attempts by the client scheduler.
SET SCHEDMODES	Specifies the central scheduling mode for the server.
SET SERVERHLADDRESS	Specifies the high-level address of a server.
SET SERVERLLADDRESS	Specifies the low-level address of a server.
SET SERVERNAME	Specifies the name by which the server is identified.
SET SERVERPASSWORD	Specifies the server password.
SET SUMMARYRETENTION	Specifies the number of days to retain information for the activity summary table.
SET TOCLOADRETENTION	Specifies the number of minutes to retain information for unreferenced TOC sets.

QUERY STATUSTHRESHOLD (Query status monitoring thresholds)

Use this command to display information about status monitoring thresholds.

Status monitoring thresholds compare the defined conditions to the status monitoring server queries and inserts the results in the status monitoring table.

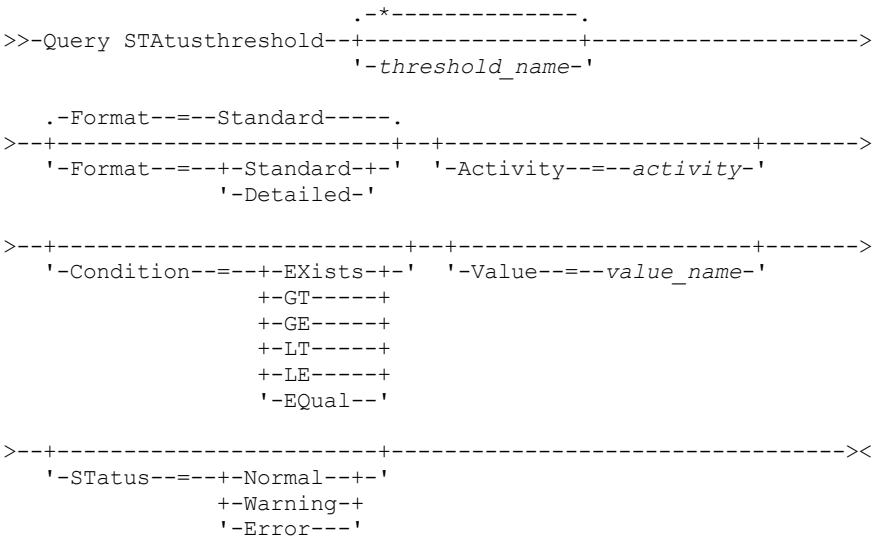
Multiple thresholds can be defined for an activity. For example, you can create a threshold that provides a warning status if storage pool capacity utilization is greater than 80%. You can then create another threshold that provides error status if storage pool capacity utilization is greater than 90%.

Note: If a threshold is already defined for an EXISTS condition, you cannot define another threshold with one of the other condition types.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

threshold_name
Specifies the threshold name. The name cannot exceed 48 characters in length.

Format
Specifies how the information is displayed. The default value is STANDARD. Possible values are:

Standard
Specifies that partial information is displayed for the specified status thresholds.

Detailed
Specifies that complete information is displayed for the specified status thresholds.

activity
Specifies the activity for which you want to display status indicators. If you do not specify a value, information is displayed for all activities. For a list of activities, see the DEFINE STATUSTHRESHOLD command.

Condition
Restricts the output to only those matching the specified value. Possible values are:

EXists
Displays status thresholds where the condition equals EXISTS.

GT
Displays status thresholds where the condition equals GT.

GE
Displays status thresholds where the condition equals GE.

LT
Displays status thresholds where the condition equals LT.

LE
Displays status thresholds where the condition equals LE.

EQual
Displays status thresholds where the condition equals EQUAL.

Value
Displays thresholds that have the specified value. If you do not specify a value, information is displayed for all values. You can specify an integer from 0 to 9223372036854775807.

STatus
Displays status thresholds that have the specified status value. If you do not specify a value, information is displayed for all values. Possible values are:

Normal
Displays the status thresholds that have a normal status value.

Warning
Displays the status thresholds that have a warning status value.

Error
Displays the status thresholds that have an error status value.

QUERY status threshold

Query all status thresholds by issuing the following command:

```
query statusthreshold
```

```
Threshold Name    Activity Name     Condition   Value     Report
                                    Name                  Status
---------------   ---------------   ---------   -------   -------
ACTIVELOGCHECK    ACTIVE LOG        >           90        ERROR
                   UTILIZATION
                   (%)
AVGSTGPLW         AVERAGE STORAGE   >           85        WARNING
                   POOL
                   UTILIZATION
                   (%)
AVGSTGPLE         AVERAGE STORAGE   >           90        ERROR
                   POOL
                   UTILIZATION
                   (%)
```

Query status thresholds and display detailed format

Query status thresholds and display the output in detailed format, by issuing the following command:

```
query statusthreshold f=d

Threshold Name: ACTIVELOGCHECK
 Activity Name: ACTIVE LOG UTILIZATION (%)
Condition Name: >
         Value: 90
 Report Status: ERROR
   Server Name: TSMAWP24

Threshold Name: AVGSTGPLW
 Activity Name: AVERAGE STORAGE POOL UTILIZATION (%)
Condition Name: >
         Value: 85
 Report Status: WARNING
   Server Name: TSMAWP24

Threshold Name: AVGSTGPLE
 Activity Name: AVERAGE STORAGE POOL UTILIZATION (%)
Condition Name: >
         Value: 95
 Report Status: ERROR
   Server Name: TSMAWP24
```

Related commands

Table 1. Commands related to QUERY STATUSTHRESHOLD

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

QUERY STGPOOL (Query storage pools)

Use this command to display information about one or more storage pools. You can also use this command to monitor migration processes for storage pools.

Privilege class

Any administrator can issue this command.

Syntax

```
                  .-*---------.  .-Format--=--Standard-----.
>>-Query STGpool--+-----------+--+-------------------------+---->
                  '-pool_name-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'

   .-POoltype--=--ANY---------------.
>--+--------------------------------+-------------------------><
   '-POoltype--=--+-ANY-----------+-'
                  +-PRimary-------+
                  +-COpy----------+
                  +-COPYCONtainer-+
                  '-ACTIVEdata----'
```

Parameters

pool_name
: Specifies the storage pool to query. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, all storage pools are displayed.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Specify one of the following values:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

POoltype
: Specifies the type of storage pool to query. This parameter is optional. The default value is ANY. Specify one of the following values:

  ANY
  : Query primary storage pools, copy storage pools, and active-data pools.

  PRimary
  : Query only primary storage pools.

  COpy
  : Query only copy storage pools.

  COPYCONtainer
  : Query only container-copy storage pools.

  ACTIVEdata
  : Query only active-data storage pools.

Example: Display detailed random-access disk storage pool information

Tip: In the examples of detailed output, some fields are blank because the item does not apply in the specified environment. Display details for a storage pool that is named DISKPOOL. See Field descriptions for field descriptions.

```
query stgpool diskpool format=detailed
```

```
                     Storage Pool Name: DISKPOOL
                     Storage Pool Type: Primary
                     Device Class Name: DISK
                          Storage Type: DEVCLASS
                            Cloud Type:
                             Cloud URL:
                        Cloud Identity:
                        Cloud Location:
                    Estimated Capacity: 66 G
                    Space Trigger Util: 0.0
                              Pct Util: 0.0
                              Pct Migr: 3.1
                           Pct Logical: 100.0
                          High Mig Pct: 90
                           Low Mig Pct: 70
                       Migration Delay: 0
                    Migration Continue: Yes
```

```
                  Migration Processes: 1
                Reclamation Processes: 1
                    Next Storage Pool:
                 Reclaim Storage Pool:
               Maximum Size Threshold: No Limit
                               Access: Read/Write
                          Description:
                     Overflow Location:
                  Cache Migrated Files?:
                             Collocate?: Group
                Reclamation Threshold: 60
            Offsite Reclamation Limit:
     Maximum Scratch Volumes Allowed: 32
      Number of Scratch Volumes Used: 1
    Delay Period for Container Reuse: 1 Day(s)
              Migration in Progress?: No
                Amount Migrated (MB): 0.00
    Elapsed Migration Time (seconds): 0
            Reclamation in Progress?: No

 Last Update by (administrator): SERVER_CONSOLE
              Last Update Date/Time: 01/03/2014 13:57:16
           Storage Pool Data Format: Native
               Copy Storage Pool(s):
                Active Data Pool(s):
            Continue Copy on Error?: No
                            CRC Data: Yes
                  Reclamation Type: Threshold
        Overwrite Data when Deleted: 2 Time(s)
                  Deduplicate Data?: No
 Processes For Identifying Duplicates:
                           Compressed:
              Deduplication Savings:
                Compression Savings:
                  Total Space Saved:
                     Auto-copy Mode: Client
Contains Data Deduplicated by Client?: No
      Maximum Simultaneous Writers:
                  Protect Processes:
           Protection Storage Pool:
      Protect Local Storage Pool(s):
           Reclamation Volume Limit:

Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
       Deduplicate Requires Backup?:
                         Encrypted:
                     Pct Encrypted:
        Cloud Space Allocated (MB):
         Cloud Space Utilized (MB):
                        Bucket Name:
          Local Estimated Capacity:
                    Local Pct Util:
                  Local Pct Logical:
```

Example: Display detailed sequential-access disk storage pool information

Display details for a storage pool that is named FILEPOOL. See Field descriptions for field descriptions.

```
query stgpool filepool format=detailed
```

```
                    Storage Pool Name: FILEPOOL
                    Storage Pool Type: Primary
                    Device Class Name: FILEC
                         Storage Type: DEVCLASS
                           Cloud Type:
                            Cloud URL:
                       Cloud Identity:
                       Cloud Location:
                  Estimated Capacity: 66 G
                  Space Trigger Util: 0.0
                            Pct Util: 0.0
                            Pct Migr: 3.1
                         Pct Logical: 100.0
```

```
                          High Mig Pct: 90
                           Low Mig Pct: 70
                       Migration Delay: 0
                    Migration Continue: Yes
                  Migration Processes: 1
                Reclamation Processes: 1
                    Next Storage Pool:
                 Reclaim Storage Pool:
               Maximum Size Threshold: No Limit
                               Access: Read/Write
                          Description:
                    Overflow Location:
                 Cache Migrated Files?:
                            Collocate?: Group
                 Reclamation Threshold: 60
            Offsite Reclamation Limit:
      Maximum Scratch Volumes Allowed: 32
        Number of Scratch Volumes Used: 1
     Delay Period for Container Reuse: 1 Day(s)
               Migration in Progress?: No
                 Amount Migrated (MB): 0.00

Elapsed Migration Time (seconds): 0
              Reclamation in Progress?: No
       Last Update by (administrator): SERVER_CONSOLE
                 Last Update Date/Time: 01/02/2014 13:57:16
            Storage Pool Data Format: Native
                Copy Storage Pool(s):
                 Active Data Pool(s):
             Continue Copy on Error?: No
                             CRC Data: Yes
                  Reclamation Type: Threshold
          Overwrite Data when Deleted:
                  Deduplicate Data?: Yes
  Processes For Identifying Duplicates: 1
                           Compressed:
                Deduplication Savings: 65,396 K (49.99%)
                  Compression Savings:
                   Total Space Saved: 65,396 K (49.99%)
                      Auto-copy Mode: Client
 Contains Data deduplicated by Client?: Yes
         Maximum Simultaneous Writers:
                   Protect Processes:
             Protection Storage Pool:
        Protect Local Storage Pool(s):
             Reclamation Volume Limit:
Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
         Deduplicate Requires Backup?:
                          Encrypted:
                      Pct Encrypted:
          Cloud Space Allocated (MB):
           Cloud Space Utilized (MB):
                          Bucket Name:
            Local Estimated Capacity:
                     Local Pct Util:
                   Local Pct Logical:
```

Example: Display detailed sequential storage pool information

Display details for an active-data sequential storage pool that is named FILEPOOL that uses a FILE type device class. See Field descriptions for field descriptions.

```
query stgpool filepool format=detailed

                   Storage Pool Name: FILEPOOL
                   Storage Pool Type: Active-data
                   Device Class Name: FILEC
                        Storage Type: DEVCLASS
                          Cloud Type:
                           Cloud URL:
                      Cloud Identity:
                      Cloud Location:
```

```
                    Estimated Capacity: 0.0 M
                    Space Trigger Util: 0.0
                              Pct Util: 0.0
                              Pct Migr: 0.0
                           Pct Logical: 0.0
                          High Mig Pct: 90
                           Low Mig Pct: 70
                       Migration Delay: 0
                    Migration Continue: Yes
                  Migration Processes: 1
                Reclamation Processes: 1
                    Next Storage Pool:
                 Reclaim Storage Pool:
              Maximum Size Threshold: No Limit
                              Access: Read/Write
                         Description:
                    Overflow Location:
                 Cache Migrated Files?:
                             Collocate?: Group
                Reclamation Threshold: 60
            Offsite Reclamation Limit:
      Maximum Scratch Volumes Allowed: 99
        Number of Scratch Volumes Used: 0
      Delay Period for Container Reuse: 1 Day(s)
                Migration in Progress?: No
                  Amount Migrated (MB): 0.00

Elapsed Migration Time (seconds): 0
             Reclamation in Progress?: No
      Last Update by (administrator): SERVER_CONSOLE
                Last Update Date/Time: 01/02/2014 11:37:57
             Storage Pool Data Format: Native
                 Copy Storage Pool(s):
                  Active Data Pool(s):
               Continue Copy on Error?:
                           CRC Data: Yes
                    Reclamation Type: Threshold
          Overwrite Data when Deleted:
                    Deduplicate Data?: Yes
  Processes For Identifying Duplicates: 1
                          Compressed:
                Deduplication Savings: 65,396 K (49.99%)
                  Compression Savings:
                    Total Space Saved: 65,396 K (49.99%)
                       Auto-copy Mode:
 Contains Data Deduplicated by Client?: No
         Maximum Simultaneous Writers:
                    Protect Processes:
              Protection Storage Pool:
        Protect Local Storage Pool(s):
             Reclamation Volume Limit:
Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                           Encrypted:
                       Pct Encrypted:
          Cloud Space Allocated (MB):
           Cloud Space Utilized (MB):
                         Bucket Name:
            Local Estimated Capacity:
                      Local Pct Util:
                   Local Pct Logical:
```

Example: Display summary information for a specific storage pool

Display information for a storage pool that is named POOL1. See Field descriptions for field descriptions.

```
query stgpool pool1

Storage     Device       Estimated  Pct  Pct   High  Low      Next
Pool Name   Class Name   Capacity   Util Migr  Mig   Mig   Storage
                                              Pct   Pct      Pool
----------  ----------   --------- ----- ----- ----  ---- --------
POOL1       DISK         58.5 M     0.8  0.7    90    70   POOL2
```

Example: Display detailed 8 mm tape storage pool information

Display details for the storage pool named 8MMPOOL. See Field descriptions for field descriptions.

```
query stgpool 8mmpool format=detailed
```

```
                      Storage Pool Name: 8MMPOOL
                      Storage Pool Type: Primary
                      Device Class Name: 8MMTAPE
                           Storage Type: DEVCLASS
                             Cloud Type:
                              Cloud URL:
                         Cloud Identity:
                         Cloud Location:
                     Estimated Capacity: 0.0 M
                     Space Trigger Util: 0.0
                               Pct Util: 0.0
                               Pct Migr:
                            Pct Logical: 0.0
                           High Mig Pct: 90
                            Low Mig Pct: 70
                        Migration Delay: 0
                     Migration Continue: Yes
                    Migration Processes: 1
                  Reclamation Processes: 1
                      Next Storage Pool:
                   Reclaim Storage Pool:
                 Maximum Size Threshold: 5 M
                                 Access: Read/Write
                            Description: Main storage pool
                       Overflow Location: Room1234/Bldg31
                   Cache Migrated Files?:
                              Collocate?: No
                  Reclamation Threshold: 60
            Offsite Reclamation Limit:
       Maximum Scratch Volumes Allowed: 5
         Number of Scratch Volumes Used: 3
      Delay Period for Container Reuse: 1 Day(s)
                Migration in Progress?: No
                  Amount Migrated (MB): 0.00

      Elapsed Migration Time (seconds): 0
              Reclamation in Progress?: No
        Last Update by (administrator): ADMIN
                 Last Update Date/Time: 01/08/2014 06:55:45
              Storage Pool Data Format: Native
                  Copy Storage Pool(s): COPYPOOL1
                   Active Data Pool(s): ACTIVEPOOL1 ACTIVEPOOL2
               Continue Copy on Error?: Yes
                               CRC Data: Yes
                     Reclamation Type: Threshold
          Overwrite Data when Deleted:
                     Deduplicate Data?: No
  Processes For Identifying Duplicates:
                           Compressed:
                Deduplication Savings:
                  Compression Savings:
                    Total Space Saved:
                           Compressed: No
                Deduplication Savings:
                  Compression Savings:
                    Total Space Saved:
                       Auto-copy Mode: Client
 Contains Data Deduplicated by Client?: No
          Maximum Simultaneous Writers:
                     Protect Processes:
               Protection Storage Pool:
        Protect Local Storage Pool(s):
             Reclamation Volume Limit:

Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                           Encrypted:
```

```
                    Pct Encrypted:
            Cloud Space Allocated (MB):
             Cloud Space Utilized (MB):
                         Bucket Name:
           Local Estimated Capacity:
                     Local Pct Util:
                  Local Pct Logical:
```

Example: Display detailed NAS2CLASS storage pool information

Display details for a storage pool, NAS2LIBPOOL. When you set up this storage pool, you set the data format to NETAPPDUMP. See Field descriptions for field descriptions.

```
query stgpool nas2libpool format=detailed
```

```
                     Storage Pool Name: NAS2
                     Storage Pool Name: NAS2LIBPOOL
                     Storage Pool Type: Primary
                     Device Class Name: NAS2CLASS
                          Storage Type: DEVCLASS
                            Cloud Type:
                             Cloud URL:
                        Cloud Identity:
                        Cloud Location:
                    Estimated Capacity: 0.0 M
                    Space Trigger Util:
                              Pct Util: 0.0
                              Pct Migr:
                           Pct Logical: 0.0
                          High Mig Pct:
                           Low Mig Pct:
                       Migration Delay:
                    Migration Continue:
                   Migration Processes:
                 Reclamation Processes:
                     Next Storage Pool:
                  Reclaim Storage Pool:
                Maximum Size Threshold:
                                Access: Read/Write
                           Description:
                      Overflow Location:
                  Cache Migrated Files?:
                             Collocate?: Group
                  Reclamation Threshold:
            Offsite Reclamation Limit:
       Maximum Scratch Volumes Allowed: 50
        Number of Scratch Volumes Used: 0
      Delay Period for Container Reuse: 1 Day(s)
               Migration in Progress?:
                 Amount Migrated (MB):

      Elapsed Migration Time (seconds):
              Reclamation in Progress?:
        Last Update by (administrator): SERVER_CONSOLE
                 Last Update Date/Time: 01/02/2014 16:24:43
              Storage Pool Data Format: NetApp Dump
                  Copy Storage Pool(s):
                   Active Data Pool(s):
               Continue Copy on Error?: No
                               CRC Data: No
                     Reclamation Type:
          Overwrite Data when Deleted:
                     Deduplicate Data?: No
  Processes For Identifying Duplicates:
                           Compressed:
                 Deduplication Savings:
                   Compression Savings:
                     Total Space Saved:
                        Auto-copy Mode: Client
 Contains Data Deduplicated by Client?: No
          Maximum Simultaneous Writers:
                     Protect Processes:
                Protection Storage Pool:
```

```
         Protect Local Storage Pool(s):
              Reclamation Volume Limit:

Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                             Encrypted:
                         Pct Encrypted:
            Cloud Space Allocated (MB):
             Cloud Space Utilized (MB):
                           Bucket Name:
              Local Estimated Capacity:
                       Local Pct Util:
                    Local Pct Logical:
```

Example: Display detailed information for a directory-container storage pool that is used for data deduplication

Display details for a directory-container storage pool, DPOOL1. See Field descriptions for field descriptions.

```
query stgpool dpool1 format=detailed

                     Storage Pool Name: DPOOL1
                     Storage Pool Type: Primary
                     Device Class Name:
                          Storage Type: Directory
                            Cloud Type:
                             Cloud URL:
                        Cloud Identity:
                        Cloud Location:
                    Estimated Capacity: 798 G
                    Space Trigger Util:
                              Pct Util: 3.4
                              Pct Migr:
                           Pct Logical: 100.0
                          High Mig Pct:
                           Low Mig Pct:
                       Migration Delay:
                    Migration Continue:
                   Migration Processes:
                 Reclamation Processes:
                     Next Storage Pool:
                  Reclaim Storage Pool:
                Maximum Size Threshold: No Limit
                                Access: Read/Write
                           Description:
                      Overflow Location:
                  Cache Migrated Files?:
                              Collocate?:
                 Reclamation Threshold:
           Offsite Reclamation Limit:
       Maximum Scratch Volumes Allowed:
        Number of Scratch Volumes Used:
      Delay Period for Container Reuse: 1 Day(s)
                Migration in Progress?:
                  Amount Migrated (MB):


      Elapsed Migration Time (seconds):
              Reclamation in Progress?:
        Last Update by (administrator): SERVER_CONSOLE
                  Last Update Date/Time: 01/02/2014 16:24:43
              Storage Pool Data Format: Native
                  Copy Storage Pool(s):
                   Active Data Pool(s):
               Continue Copy on Error?:
                               CRC Data: No
                     Reclamation Type:
          Overwrite Data when Deleted:
                     Deduplicate Data?: Yes
  Processes For Identifying Duplicates:
                           Compressed: Yes
         Space Used for Protected Data: 1,599 M
```

```
                  Total Pending Space: 100 M
                Deduplication Savings: 1,331 M (67.56%)
                  Compression Savings: 194,805 K (29.82%)
                    Total Space Saved: 1,521 M (77.22%)
                       Auto-copy Mode:
 Contains Data Deduplicated by Client?:
          Maximum Simultaneous Writers: No Limit
                     Protect Processes:
               Protection Storage Pool: DPOOL2
         Protect Local Storage Pool(s):
              Reclamation Volume Limit:

Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                           Encrypted:
                       Pct Encrypted: 34.56%
            Cloud Space Allocated (MB):
             Cloud Space Utilized (MB):
                         Bucket Name:
           Local Estimated Capacity:
                     Local Pct Util:
                   Local Pct Logical:
```

Example: Display detailed information for a cloud-container storage pool that is used for data deduplication

Display details for a cloud container storage pool, CPOOL1. See Field descriptions for field descriptions.

```
query stgpool cpool1 format=detailed

                     Storage Pool Name: CPOOL1
                     Storage Pool Type: Primary
                     Device Class Name:
                          Storage Type: CLOUD
                            Cloud Type: SWIFT
                             Cloud URL: http://localhost.local
                        Cloud Identity: Bailey
                        Cloud Location: ONPREMISE
                    Estimated Capacity:
                    Space Trigger Util:
                              Pct Util:
                              Pct Migr:
                           Pct Logical: 0.0
                          High Mig Pct:
                           Low Mig Pct:
                       Migration Delay:
                    Migration Continue:
                   Migration Processes:
                 Reclamation Processes:
                     Next Storage Pool:
                  Reclaim Storage Pool:
                Maximum Size Threshold: No Limit
                               Access: Read/Write
                           Description:
                      Overflow Location:
                  Cache Migrated Files?:
                               Collocate?:
                 Reclamation Threshold:
               Offsite Reclamation Limit:
        Maximum Scratch Volumes Allowed:
         Number of Scratch Volumes Used:
          Delay Period for Volume Reuse: 1
                 Migration in Progress?:
                   Amount Migrated (MB):

       Elapsed Migration Time (seconds):
                Reclamation in Progress?:
          Last Update by (administrator): CODY
                   Last Update Date/Time: 2015-05-28, 10:47:52
                Storage Pool Data Format: Native
                    Copy Storage Pool(s):
```

```
                  Active Data Pool(s):
              Continue Copy on Error?:
                             CRC Data: No
                     Reclamation Type:
          Overwrite Data when Deleted:
                     Deduplicate Data?: Yes
  Processes For Identifying Duplicates:
                           Compressed: Yes
                Deduplication Savings: 9,241 K (89.76%)
                  Compression Savings: 1,033 K (98.81%)
                    Total Space Saved: 10,274 K (99.79%)
                       Auto-copy Mode:
 Contains Data Deduplicated by Client?:
          Maximum Simultaneous Writers: No Limit
                     Protect Processes:
               Protection Storage Pool:
         Protect Local Storage Pool(s):
              Reclamation Volume Limit:

Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                           Encrypted: Yes
                       Pct Encrypted: 34.56%
            Cloud Space Allocated (MB): 4,231
             Cloud Space Utilized (MB): 4,231
                         Bucket Name:
              Local Estimated Capacity: 168 G
                        Local Pct Util: 0.1
                     Local Pct Logical: 100.0
```

Field descriptions

Storage Pool Name
: The name of the storage pool.

Storage Pool Type
: The type of storage pool.

Device Class Name
: The name of the device class that is assigned to the storage pool.

Storage Type
: The type of storage that is defined for the storage pool. The following storage types can be shown:

  DEVCLASS
  : The storage pool specifies a device class, which determines the type of device where data is stored.

  DIRECTORY
  : The storage pool creates logical containers for data in file system directories.

  CLOUD
  : The storage pool creates logical containers for data in a cloud environment.

Cloud Type
: For cloud storage pools, the type of cloud platform.

Cloud URL
: For cloud storage pools, the URL for accessing the on-premises private cloud or off-premises public cloud.

Cloud Identity
: For cloud storage pools, the user ID for accessing the on-premises private cloud or off-premises public cloud.

Cloud Location
: For cloud storage pools, indicates whether the cloud is an on-premises private cloud or off-premises public cloud.

Estimated Capacity
: The estimated capacity of the storage pool in megabytes (M) or gigabytes (G).

  For DISK devices, estimated capacity is the capacity of all volumes in the storage pool, including any volumes that are varied offline.

  For sequential-access storage pools, estimated capacity is the total estimated space of all the sequential-access volumes in the storage pool, regardless of their access mode. At least one volume must be used in a sequential-access storage pool (either a scratch volume or a private volume) to calculate estimated capacity.

For tape and FILE devices, the estimated capacity for the storage pool includes the following factors:

- The capacity of all the scratch volumes that the storage pool already acquired or can acquire. The number of scratch volumes is defined by the MAXSCRATCH parameter on the DEFINE STGPOOL or UPDATE STGPOOL command.
- The total number of available scratch volumes in the tape library.
- Estimated capacity is the smaller number between the MAXSCRATCH value and the total number of available scratch volumes in the tape library.

The calculations for estimated capacity depend on the available space of the storage for the device that is assigned to the storage pool. For FILE storage pools, the capacity for the storage pool is reduced if the available storage is less than the total estimated space of all the FILE volumes in the storage pool. The value that is displayed for capacity is reduced by the size of a FILE volume incrementally as the available space continues to decline.

For Centera, value represents the total capacity of the Centera storage device that is being queried.

Space Trigger Util
: Utilization of the storage pool, as calculated by the storage pool space trigger, if any, for this storage pool. You can define space triggers for storage pools that are associated with DISK or FILE device types only.

  For sequential access devices, space trigger utilization is expressed as follows as a percentage of the number of used bytes on each sequential access volume relative to the size of the volume and estimated capacity of all existing volumes in the storage pool. It does not include potential scratch volumes. Unlike the calculation for percent utilization, the calculation for space trigger utilization favors creation of new private file volumes by the space trigger over usage of more scratch volumes.

  For disk devices, space trigger utilization is expressed as a percentage of the estimated capacity, including cached data. However, it excludes data that is on any volumes that are varied offline. The value for space trigger utilization can be higher than the value for percent migration if you issue QUERY STGPOOL while a file creation is in progress. The value for space trigger utilization is determined by the amount of space that is allocated while the transaction is in progress. The value for percent migration represents only the space that is occupied by committed files. At the end of the transaction, these values are synchronized.

  The value for space trigger utilization includes cached data on disk volumes. Therefore, when cache is enabled and migration occurs, the value remains the same because the migrated data remains on the volume as cached data. The value decreases only when the cached data expires or when the space that cached files occupy must be used for noncached files.

Pct Util
: An estimate of the utilization of the storage pool, as a percentage.

  For sequential access devices, it is a percentage of the number of active bytes on each sequential access volume and the estimated capacity of all volumes in the storage pool. The percentage includes the number of potential scratch volumes that might be allocated.

  For disk devices, it is a percentage of the estimated capacity, including cached data and data that is on any volumes that are varied offline. The value for Pct Util can be higher than the value for Pct Migr if you issue this command while a file creation transaction is in progress. The value for Pct Util is determined by the amount of space that is allocated, while the transaction is in progress. The value for Pct Migr represents only the space that is occupied by committed files. At the end of the transaction, these values become synchronized.

  The Pct Util value includes cached data on disk volumes. Therefore, when cache is enabled and migration occurs, the Pct Util value remains the same because the migrated data remains on the volume as cached data. The Pct Util value decreases only when the cached data expires or when the space that cached files occupy must be used for noncached files.

  For Centera, this represents an estimate of the utilization of the entire Centera storage device, not the storage pool that is being queried.

Pct Migr (primary storage pools only)
: An estimate of the percentage of data in the storage pool that can be migrated. The server uses this value and the high and low migration thresholds to determine when to start and stop migration.

  For random-access disk devices, this value is specified as a percentage of the value for the estimated capacity, excluding cached data, but including data on any volumes varied offline.

  For sequential-access disk devices, this value is specified as a percentage of the value for the estimated capacity. The value includes the capacity of all the scratch volumes that are specified for the pool. For other types of sequential-access

devices, this value is the percentage of the total number of volumes in the pool that contain at least one byte of active data. The total number of volumes includes the maximum number of scratch volumes.

The Pct Util value includes cached data on a volume; the Pct Migr value excludes cached data. Therefore, when cache is enabled and migration occurs, the Pct Migr value decreases but the Pct Util value remains the same because the migrated data remains on the volume as cached data. The Pct Util value decreases only when the cached data expires or when the space that cached files occupy must be used for noncached files.

Pct Logical
: The logical occupancy of the storage pool as a percentage of the total occupancy. Logical occupancy is space that is occupied by client files that might or might not be part of an aggregate. A Pct Logical value less than 100% indicates that there is vacant space within aggregates in the storage pool.

High Mig Pct (primary storage pools only)
: The high migration threshold, which specifies when the server can begin migration for the storage pool. The server starts migration processes when capacity utilization reaches this threshold.

Low Mig Pct (primary storage pools only)
: The low migration threshold, which specifies when the server can stop migration for the storage pool. The server stops migration processes when capacity utilization reaches this threshold.

Migration Delay (primary storage pools only)
: The minimum number of days that a file must remain in a storage pool before the server can migrate the file to the next storage pool. For a disk storage pool, the days are counted from the time that the file was stored in the storage pool or last retrieved by a client. For a sequential access storage pool, the days are counted from the time that the file was stored in the storage pool.

Migration Continue (primary storage pools only)
: Whether the server continues to migrate files to the next storage pool even if the files have not been in the pool for the number of days that are specified by the migration delay.

Migration Processes
: The number of parallel processes that are used for migrating files from a random or sequential access primary storage pool.

Reclamation Processes
: The number of parallel processes that are used for reclaiming the volumes in a sequential access primary or copy storage pool.

Next Storage Pool (primary storage pools only)
: The storage pool that is the destination for data that is migrated from this storage pool.

Reclaim Storage Pool (primary, sequential access storage pools only)
: If specified, the storage pool that is the destination for data that is moved from volumes during reclamation processing. If no pool is specified, by default reclamation processing moves data only among volumes within the same storage pool.

Maximum Size Threshold (primary storage pools only)
: The maximum size of files that might be stored in the storage pool.

Access
: The access mode for data in the storage pool. The following access modes are possible:

  Read/Write
  : The data can be accessed in read-write mode.

  Read only
  : The data can be accessed in read-only mode.

  Converting
  : The storage pool is being converted to a directory-container storage pool.

  Conversion Stopped
  : The process of converting the storage pool to a directory-container storage pool is stopped.

  Conversion Cleanup Needed
  : To convert the storage pool successfully, you must clean up the storage pool. Conversion could not complete because of damaged data. Issue the QUERY CLEANUP command to identify damaged files.

  Converted
  : The storage pool is converted to a directory-container storage pool.

Description
: The description of the storage pool.

Overflow Location (sequential access storage pools only)
: The location where volumes in the storage pool are stored when they are ejected from an automated library with the MOVE MEDIA command.

Cache Migrated Files? (random access storage pools only)
: Whether caching is enabled for files that are migrated to the next storage pool.

Collocate? (sequential access storage pools only)

Whether collocation is disabled or enabled. If collocation is disabled, the value of this field is No. If collocation is enabled, the possible values are Group, Node, and File space.

Reclamation Threshold (sequential access storage pools only)
: The threshold that determines when volumes in a storage pool are reclaimed. The server compares the percentage of reclaimable space on a volume to this value to determine whether reclamation is necessary.

Offsite Reclamation Limit
: The number of offsite volumes that have space that is reclaimed during reclamation for this storage pool. This field applies only when POOLTYPE=COPY.

Maximum Scratch Volumes Allowed (sequential access storage pools only)
: The maximum number of scratch volumes that the server can request for the storage pool.

Number of Scratch Volumes Used (sequential access storage pools only)
: The number of scratch volumes that are used in the storage pool.

Delay Period for Container Reuse (container storage pools only)
: The number of days that must elapse after all files are deleted from a container before the server reuses the container.

Migration in Progress? (primary storage pools only)
: Whether at least one migration process is active for the storage pool.

Amount Migrated (MB) (primary storage pools only)
: The amount of data, in megabytes, that is migrated, if migration is in progress. If migration is not in progress, this value indicates the amount of data that was migrated during the last migration. When multiple, parallel migration processes are used for the storage pool, this value indicates the total amount of data that is migrated by all processes.

Elapsed Migration Time (seconds) (primary storage pools only)
: The amount of time that elapsed since migration began, if migration is active. If migration is not active, this value indicates the amount of time that is required to complete the last migration. When multiple, parallel migration processes are used for the storage pool, this value indicates the total time from the beginning of the first process until the completion of the last process.

Reclamation in Progress? (sequential access storage pools only)
: Whether a reclamation process is active for the storage pool.

Last Update by (administrator)
: The name of the administrator that is defined or most recently updated the storage pool.

Last Update Date/Time
: The date and time that an administrator defined or most recently updated the storage pool.

Storage Pool Data Format
: The type of data format that is used to write data to this storage pool (for example NATIVE, NETAPPDUMP, CELERRADUMP, or NDMPDUMP).

Copy Storage Pool(s)
: The copy storage pools that are listed have data that is simultaneously written to them when data is backed up or archived to the primary storage pool queried by this command.

Active Data Pool(s)
: The active-data pools that are listed here have data that is simultaneously written to them when data is backed up to the primary storage pool queried by this command.

Continue Copy on Error?
: Whether a server continues to write data to other copy storage pools in the list or ends the entire transaction when a write failure occurs to one of the copy pools in the list. This field applies only to primary random-access and primary sequential-access storage pools.

CRC Data
: Whether data is validated by a cyclic redundancy check (CRC) when data is transferred during data storage and retrieval on a device.

Reclamation Type
: Whether volumes in this storage pool are reclaimed by threshold or by SnapLock retention date.

Overwrite Data when Deleted
: The number of times data will be physically overwritten after it is deleted from the database.

Deduplicate Data?
: Whether data in the storage pool is deduplicated.

Processes for Identifying Duplicates
: The number of duplicate-identification processes that are specified as the default for the storage pool. The number of duplicate-identification processes that are specified in this field might not equal the number of duplicate-identification processes that are running.

Compressed
: Whether the storage pool is compressed.

Additional space for protected data

The amount of space, in MB, that is used to protect data from remote servers. This is the total amount of space used for data received from other servers as a result of running the PROTECT STGPOOL command.

After the PROTECT STGPOOL command is run, the data is not assigned to a node. However, if you run node replication on some or all nodes, then the data is assigned to the nodes and is no longer assigned to the additional space for protected data.

If you do not run node replication, then the data received (after the PROTECT STGPOOL command is run) remains assigned to the additional space for protected data.

Total Unused Pending Space
: The amount of space that is scheduled to become available in a directory-container storage pool. The space is occupied by deduplicated data extents that will be removed from the storage pool when the time period specified by the REUSEDELAY parameter on the DEFINE STGPOOL command expires.

Deduplication Savings
: The amount and percentage of data that is saved in the storage pool by using data deduplication.

Compression Savings
: The amount of data that is saved in the storage pool by compression.

Total Space Saved
: The total amount of data that was saved in the storage pool.

Auto-copy Mode
: Indicates whether data is written simultaneously to copy storage pools or active-data pools during client store sessions, server import processes, server data migration processes, or all three operations. The value CLIENT indicates either client store or server import operations. The value ALL indicates that simultaneous-write operations occur whenever this pool is a target for any of the eligible operations.

  If the storage pool is a copy storage pool or an active-data pool or if the simultaneous-write function is disabled, this field is blank.

Contains Data Deduplicated by Client?
: Indicates whether the storage pool contains data that was deduplicated by clients. Storage pools that contain data that is deduplicated by clients are not accessible for LAN-free data movement by storage agents V6.1 or earlier.
  Tip: This field is blank for container storage pools. You cannot use container storage pools for LAN-free data movement.

Maximum Simultaneous Writers
: The maximum number of I/O that can run concurrently on the storage pool.

Protect Processes
: The set of protect processes.

Protection Storage Pool
: The name of the container storage pool where the data is protected to on the target replication server.

Protect Local Storage Pool(s)
: Indicates whether local storage pools are protected.

Reclamation Volume Limit
: For container-copy storage pools, indicates the maximum number of volumes that the server reclaims during storage pool protection.

Date of Last Protection to Remote Pool
: The date that the storage pool was last protected to a storage pool on a remote server.

Date of Last Protection to Local Pool
: The date that the storage pool was last protected to a storage pool on the local server.

Deduplicate Requires Backup?
: Indicates whether the sequential storage pool must be backed up if the storage pool contains deduplicated data.

Encrypted
: For directory-container or cloud-container storage pools, indicates whether client data is encrypted before it is written to the storage pool.

Pct Encrypted
: The percentage of deduplicated client data that is encrypted in the directory-container or cloud-container storage pool.

Cloud Space Allocated (MB)
: For cloud storage pools, the amount of space that is allocated to cloud storage, in megabytes.

Cloud Space Utilized (MB)
: For cloud storage pools, the space that is used by the cloud storage, in megabytes.

Bucket Name
: For cloud storage pools that use Simple Storage Service (S3), the name IBM Spectrum Protect™ assigns to the S3 bucket or IBM® Cloud Object Storage vault. This value can also be the name that you assigned to the bucket by using the BUCKETNAME parameter in the DEFINE STGPOOL command or the UPDATE STGPOOL command.

Local Estimated Capacity
: For cloud storage pools that use local storage, the estimated capacity of the local storage in megabytes (M) or gigabytes (G).

Local Pct Util
: For cloud storage pools that use local storage, an estimate of the utilization of the local storage component of the cloud storage pool, as a percentage.

Local Pct Logical
: For cloud storage pools that use local storage, the logical occupancy of the cloud storage pool as a percentage of the total occupancy. Logical occupancy is space that is occupied by client files that might or might not be part of an aggregate. A Local Pct Logical value less than 100% indicates that there is vacant space within aggregates in the cloud storage pool.

Related commands

Table 1. Commands related to QUERY STGPOOL

Command	Description
CONVERT STGPOOL	Convert a storage pool to a directory-container storage pool.
COPY ACTIVEDATA	Copies active backup data.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE STGPOOL	Deletes a storage pool from server storage.
QUERY STGPOOLDIRECTORY	Displays information about storage pool directories.
UPDATE STGPOOL	Changes the attributes of a storage pool.

AIX Linux Windows

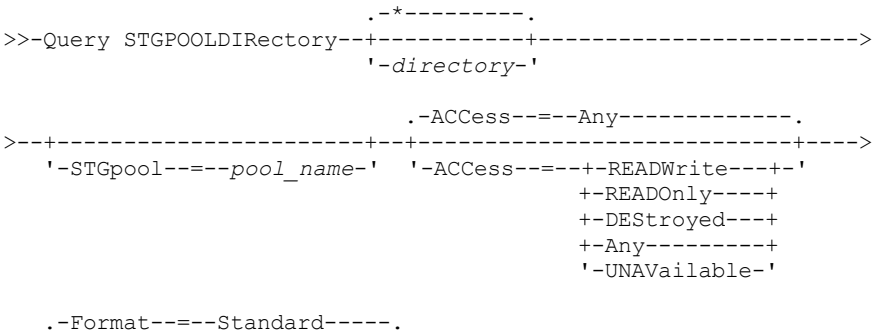
QUERY STGPOOLDIRECTORY (Query a storage pool directory)

Use this command to display information about one or more storage pool directories.

Privilege class

Any administrator can issue this command.

Syntax



```
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

directory
: Specifies the storage pool directory to query. This parameter is optional.

  *
  : Specifies that an asterisk (*) represents a wildcard character. Use wildcard characters such as an asterisk to match any characters. Alternatively, you can use a question mark (?) or a percent sign (%) to match exactly one character. This is the default.

  directory
  : Specifies the storage pool directory. If you do not specify a value for this parameter, all storage pool directories are displayed. The maximum length of the storage pool directory is 1024.

STGpool
: Specifies the name of the storage pool to query. If you do not specify a value for this parameter, all storage pool directories are displayed. The maximum length of the storage pool name is 30. This parameter is optional.

ACCess
: Specifies that output is restricted by directory access mode. This parameter is optional. Specify one of the following values:

  READWrite
  : Display all storage pool directories with an access mode of `READWRITE`.

  READOnly
  : Display all storage pool directories with an access mode of `READONLY`.

  DEStroyed
  : Display all storage pool directories with an access mode of `DESTROYED`. The directories are designated as permanently damaged in the storage pool directory.

  Any
  : Display all storage pool directories. This is the default.

  UNAVailable
  : Display directories with an access mode of `UNAVAILABLE`.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. You can specify one of the following values:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

Example: Display summary information for a specific storage pool directory

Display information for the storage pool directory that is named DPOOL. See Field descriptions for field descriptions.

```
query stgpooldirectory C:\data
```

```
Storage     Directory     Access
Pool Name
----------  ----------   ---------
DPOOL       C:\data       Read/Write
```

Example: Display detailed storage pool directory information

Display details for the storage pool directory named that is named DPOOL.

```
query stgpooldirectory stgpool=dpool format=detailed
```

AIX | Linux

```
Storage Pool Name: DPOOL
        Directory: /storage/sampleDir
           Access: Read/Write
   Free Space(MB): 323,170
  Total Space(MB): 476,938
      File System: /storage
    Absolute Path: /storage/data
```

Windows

```
Storage Pool Name: DPOOL
        Directory: /storage2/sampleDir
           Access: Read/Write
   Free Space(MB): 323,170
  Total Space(MB): 476,938
      File System: /storage
    Absolute Path: /storage2/sampleDir
```

Field descriptions

Storage Pool Name
: The name of the storage pool.

Directory
: The name of the storage pool directory.

Access
: The access mode of the data in the storage pool directory.

Free Space (MB)
: The amount of space in the storage pool directory, in megabytes, that is not in use.

Total Space (MB)
: The total amount of space in the storage pool directory, in megabytes.

File System
: The name of the file system where the storage pool directory is located.

Absolute Path
: The absolute path name where the storage pool directory is located. The absolute path name contains the name of the root directory and all subdirectories in the path name. All symbolic links are resolved in the absolute path name.

Table 1. Commands related to QUERY STGPOOLDIRECTORY

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
AIX Linux Windows DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
AIX Linux Windows DELETE STGPOOLDIRECTORY	Deletes a storage pool directory from a directory-container or cloud-container storage pool.
AIX Linux Windows UPDATE STGPOOLDIRECTORY	Changes the attributes of a storage pool directory.

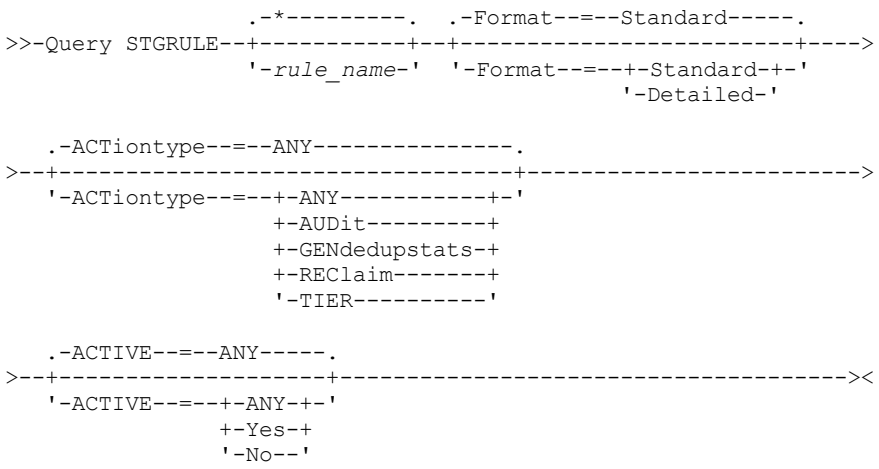
QUERY STGRULE (Display storage rule information)

Use this command to display information about storage rules that are defined for storage pools.

Privilege class

Any administrator can issue this command.

Syntax



Parameters

rule_name
: Specifies the name of one or more storage rules. This parameter is optional. You can use wildcard characters to specify this name. If you do not specify a value for this parameter, all storage rules are displayed. The maximum length of the name is 30 characters.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. The following values are possible:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

ACTiontype
: Specifies the storage action that is completed by the storage rules. The following values are possible:

  ANY
  : All types of storage rules are displayed.

  AUDit
  : Storage rules for audit operations are displayed.

  GENdedupstats
  : Storage rules for data deduplication statistics are displayed.

  RECLaim
  : Storage rules for reclaiming cloud-container storage pools are displayed.

  TIER
  : Storage rules for tiering are displayed.

ACTIVE
: Specifies whether active or inactive storage rules are displayed. This parameter is optional. The default is ANY. The following values are possible:

  ANY
  : Specifies that all storage rules are displayed.

  Yes
  : Specifies that only active storage rules are displayed.

  No
  : Specifies that only inactive storage rules are displayed.

Example: List all storage rules for all storage pools

Tip: In the output examples, some fields are blank because the item does not apply in the specified environment.
Query all storage rules for all storage pools. See QUERY STGRULE (Display storage rule information) for field descriptions.

```
query stgrule
```

```
Storage      Target Storage   Action   Active        Source Storage
Rule         Pool             Type                   Pools
Name
---------     ---------    ------     ---------     ------------------------
STGACTION1     CLOUD        Tier        Yes           DIRPOOL1
```

Example: Display detailed information about a storage rule for tiering

Query detailed information about a storage rule for tiering. See QUERY STGRULE (Display storage rule information) for field descriptions.

```
query stgrule format=detailed

       Storage Rule Name: RULE1
     Target Storage Pool: CLOUD1
             Action Type: Tier
                  Active: Yes
       Maximum Processes: 8
              Start Time: 18:00:00
         Delay (in days): 30
                Duration:
             Description:
              Audit Type:
             Audit Level:
               Node Name:
         Filespace names:
                Name Type:
                Code Type:
            Percent Unused:
      Last Exe Date/Time:
    Source Storage Pools: DIRPOOL1
```

Example: Display detailed information about a storage rule for auditing storage pools

Query detailed information about a storage rule for auditing storage pools. See QUERY STGRULE (Display storage rule information) for field descriptions.

```
query stgrule format=detailed

          Storage Rule Name: AUDIT
        Target Storage Pool: CTR
                Action Type: Audit
                     Active: Yes
          Maximum Processes: 4
                 Start Time: 11:42:36
            Delay (in days): 7
                   Duration:
                Description:
                 Audit Type: Extent
                Audit Level: 5
                  Node Name:
            Filespace names:
                  Name Type:
                  Code Type:
             Percent Unused:
          Last Exe Date/Time: 01/19/2018 11:43:31
        Source Storage Pools:
```

Example: Display detailed information about a storage rule for generating data deduplication statistics

Query detailed information about a storage rule for generating data deduplication statistics. See QUERY STGRULE (Display storage rule information) for field descriptions.

```
query stgrule format=detailed

       Storage Rule Name: GEN1
     Target Storage Pool: DIRPOOL
             Action Type: GenDedupStats
                  Active: Yes
       Maximum Processes: 8
```

```
             Start Time: 12:06:46
         Delay (in days): 1
                Duration:
             Description:
              Audit Type:
             Audit Level:
               Node Name: *
         Filespace names: *
               Name Type: SERVER
               Code Type: BOTH
    Last Exe Date/Time: 01/18/2018 12:07:10
  Source Storage Pools:
```

Example: Display detailed information about a storage rule for reclaiming space in cloud-container storage pools

Query detailed information about a storage rule for reclaiming space in cloud-container storage pools. See QUERY STGRULE (Display storage rule information) for field descriptions.

```
query stgrule format=detailed
```

```
       Storage Rule Name: RECLAIM
    Target Storage Pool: CLOUD1
            Action Type: Reclaim
                 Active: Yes
      Maximum Processes: 8
             Start Time: 9:04:16
        Delay (in days):
                Duration: 120
             Description:
              Audit Type:
             Audit Level:
               Node Name: *
         Filespace names: *
               Name Type:
               Code Type:
          Percent Unused: 50
    Last Exe Date/Time: 01/30/2018 12:07:10
  Source Storage Pools:
```

Field descriptions

Storage Rule Name
: The name of the storage rule.

Target Storage Pool
: The name of the target storage pool.

Action Type
: The type of storage rule.

Active
: Indication of whether the storage rule is active or inactive.

Maximum Processes
: The number of maximum processes per storage pool.
  Tip: For tiering storage rules, this value specifies the maximum number of processes for the source storage pool. For audit storage rules, you cannot set a maximum process value. The server automatically sets and adjusts the number of maximum processes during audit operations.

Start Time
: The starting time of the window when the storage rule runs.

Delay (in days)
: The number of days to wait before the storage rule operation occurs. For audit storage rules, the number represents the interval, in days, between audit operations. For tiering storage rules, the number represents the minimum number of days that an object must remain in a source storage pool before it is moved to a target storage pool.

Duration
: The number of minutes that the storage rule processes the data when all associated processes are completed. No value indicates that processing continues until complete.

Description
: A description of the storage rule.

Audit Type

The type of audit operation.

Audit Level
: The level of audit operation.

Filespace names
: The names of one or more affected file spaces.

Name Type
: Indication of how the server interprets file space names.

Code Type
: Indicates the type of file spaces that are included.

Percent Unused
: Specifies the percentage of unused space in reclamation storage rules.

Last Exe Date/Time
: Specifies the last date and time when the storage rule was run.

Source Storage Pools
: The name of the source storage pool or pools.

Related commands

Table 1. Commands related to QUERY STGRULE

Command	Description
DEFINE STGRULE (auditing)	Defines a storage rule for auditing storage pools.
DEFINE STGRULE (data deduplication statistics)	Defines a storage rule for generating data deduplication statistics.
DEFINE STGRULE (reclaiming)	Defines a storage rule for reclaiming cloud-container storage pools.
DEFINE STGRULE (tiering)	Defines a storage rule for tiering.
DELETE STGRULE	Deletes storage rules.
UPDATE STGRULE (auditing)	Updates a storage rule for auditing storage pools.
UPDATE STGRULE (data deduplication statistics)	Updates a storage rule for generating data deduplication statistics.
UPDATE STGRULE (reclaiming)	Updates a storage rule for reclaiming cloud-container storage pools.
UPDATE STGRULE (tiering)	Updates a tiering storage rule.

QUERY SUBSCRIBER (Display subscriber information)

Use this command on a configuration manager to display information about subscribers and their profile subscriptions.

Privilege class

Any administrator can issue this command.

Syntax

```
                      .-*-----------.
>>-Query SUBSCRIBer--+-------------+--------------------------->
                      '-server_name-'

   .-PROFIle--=--*------------.
>--+--------------------------+-------------------------------><
   '-PROFIle--=--profile_name-'
```

Parameters

server_name

Specifies the name of a managed server for which subscription information is displayed. You can use wildcard characters to specify multiple server names. This parameter is optional. The default is all managed servers.

PROFIle

Specifies a profile name for which information is displayed. You can use wildcard characters to specify multiple profile names. This parameter is optional. The default is all profiles.

Example: List a configuration manager's profile subscriptions

Display subscriber information for all profile subscriptions to this configuration manager. See Field descriptions for field descriptions.

```
query subscriber

Subscriber        Profile name       Is current?    Last update
                                                    date/time
---------------   ---------------    ------------   -----------------
SERVER2           DEFAULT_PROFILE    Yes            Thu, May 14, 1998
                                                    01:14:42 PM
SERVER2           SETUP              Yes            Thu, May 14, 1998
                                                    01:14:42 PM
```

Field descriptions

Subscriber

The name of the subscriber (managed server).

Profile name

The name of the profile.

Is current?

Whether the subscription has been refreshed with the current information associated with the profile. Possible values are:

Yes

The managed server is current.

No

The managed server is not current. If this field is NO after the profile has been refreshed, check the server messages for error conditions that might cause the refresh to fail.

Unknown

Either the managed server has a more recent version of the profile than the configuration manager, or the profile no longer exists on the configuration manager, but the subscription is still associated with the profile.

Last update date/time

Specifies the date and time that configuration information for the subscription was successfully distributed to the subscriber.

Related commands

Table 1. Commands related to QUERY SUBSCRIBER

Command	Description
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
QUERY SUBSCRIPTION	Displays information about profile subscriptions.

QUERY SUBSCRIPTION (Display subscription information)

Use this command on a managed server to display profile subscription information.

Privilege class

Any administrator can issue this command.

Syntax

```
                        .-*------------.
>>-Query SUBSCRIPtion--+--------------+------------------------><
                        '-profile_name-'
```

Parameters

profile_name
: Specifies the name of the profile for which subscription information is displayed. You can use wildcard characters to specify multiple names. This parameter is optional. The default is all profiles.

Example: Display description information

Display subscription information for all profiles.

```
query subscription

Configuration       Profile name          Last update
manager                                   date/time
---------------     ---------------       ---------
SERVER1             ADMIN_INFO            Thu, May 14, 1998
                                          01:35:13 PM
SERVER1             DEFAULT_PROFILE       Thu, May 14, 1998
                                          01:35:13 PM
SERVER1             EMPLOYEE              Thu, May 14, 1998
                                          01:35:13 PM
```

Field descriptions

Configuration manager
: The name of the configuration manager.

Profile name
: The name of the profile.

Last update date/time
: When the most recent configuration information was successfully distributed to the subscriber.

Related commands

Table 1. Commands related to QUERY SUBSCRIPTION

Command	Description
DEFINE SUBSCRIPTION	Subscribes a managed server to a profile.
DELETE SUBSCRIBER	Deletes obsolete managed server subscriptions.
DELETE SUBSCRIPTION	Deletes a specified profile subscription.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
QUERY SUBSCRIBER	Displays information about subscribers and their subscriptions to profiles.

QUERY SYSTEM (Query the system configuration and capacity)

Use this command to obtain consolidated information about the server's configuration and capacity.

This command consolidates output from select statements, SHOW commands, and other IBM Spectrum Protect™ commands. Output is generated from several IBM Spectrum Protect commands, for example:

- QUERY ASSOCIATION
- QUERY COPYGROUP

- QUERY DATAMOVER
- QUERY DB
- QUERY DBSPACE
- QUERY DEVCLASS
- QUERY DIRSPACE
- QUERY DOMAIN
- QUERY LIBRARY
- QUERY LOG
- QUERY MGMTCLASS
- QUERY OPTION
- QUERY PROCESS
- QUERY REPLRULE
- QUERY SCHEDULE
- QUERY SERVER
- QUERY SESSION
- QUERY STATUS
- QUERY STGPOOL
- QUERY VOLHISTORY
- QUERY VOLUME

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query SYStem-----------------------------------------------><
```

Example: View consolidated system information

Issue the QUERY SYSTEM command to obtain consolidated system information. For sample outputs for these query commands, see the individual commands.

```
query system
```

Related commands

Table 1. Commands related to QUERY SYSTEM

Command	Description
QUERY ASSOCIATION	Displays the clients associated with one or more schedules.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY DB	Displays allocation information about the database.
QUERY DBSPACE	Displays information about the storage space defined for the database.
QUERY DEVCLASS	Displays information about device classes.
QUERY DOMAIN	Displays information about policy domains.
QUERY LOG	Displays information about the recovery log.
QUERY MGMTCLASS	Displays information about management classes.
QUERY OPTION	Displays information about server options.
QUERY PROCESS	Displays information about background processes.
QUERY SCHEDULE	Displays information about schedules.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
QUERY STGPOOL	Displays information about storage pools.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
QUERY VOLUME	Displays information about storage pool volumes.

QUERY TAPEALERTMSG (Display status of SET TAPEALERTMSG command)

Use this command to display the status of the SET TAPEALERTMSG command. You can enable or disable tape alerts. When enabled, IBM Spectrum Protect™ can retrieve diagnostic information from a tape or library device and display it using ANR messages. When disabled, IBM Spectrum Protect will not query a device for this information.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-Query TAPEAlertmsg----------------------------------------><
```

Example: Display the status of the QUERY TAPEALERTMSG command

Use the QUERY TAPEALERTMSG command to determine if tape alerts are to be retrieved from devices and displayed in the form of ANR messages.

```
query tapealertmsg

ANR2017I Administrator SERVER_CONSOLE issued command:
         QUERY TAPEALERTMSG
ANR8960I QUERY TAPEALERTMSG: The display of Tape Alerts from SCSI
         devices is Enabled.
```

Related commands

Table 1. Commands related to QUERY TAPEALERTMSG

Command	Description
SET TAPEALERTMSG	Specifies whether tape and library devices report diagnostic information to the server.

QUERY TOC (Display table of contents for a backup image)

Use this command to display directory and file information contained in the table of contents (TOC) for a specified backup image. This command does not load table of contents information into the IBM Spectrum Protect™ database. The specified table of contents are read from a storage pool each time the QUERY TOC command is issued.

This command cannot be issued from the server console. If the table of contents is stored on removable media, a mount point is required and output is delayed while the storage pool volume is mounted.

Privilege class

To issue this command you must have either system privilege, policy privilege for the domain to which the node is assigned, or client owner authority over the node.

Syntax

```
>>-Query TOC--node_name--filespace_name------------------------->

>--+-----------------------------------------------+------------>
   '-CREATIONDate--=--date--CREATIONTime--=--time-'

   .-Format--=--Standard-----.
>--+-------------------------+-------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameters

node_name (Required)
: Specifies the name of the NAS node to which the table of contents (TOC) belongs. You cannot use wildcards to specify this name.

filespace_name (Required)
: Specifies the name of the file space to which the table of contents belongs. The file space name you specify cannot contain wildcard characters.

CREATIONDate
: Specifies the creation date of the backup image for which the table of contents is to be displayed. This parameter is optional. If you specify CREATIONDATE, you must also specify CREATIONTIME. If you do not specify these parameters, the contents of the latest backup image for the specified node and file space will be displayed, provided that this image has a table of contents. You can only specify the creation date as the following:

Value	Description	Example
MM/DD/YYYY	A specific date	05/15/2002

This specifies that you want to display the contents of the backup image created on this date. You can obtain this date from the output of the QUERY NASBACKUP command.

CREATIONTime
: Specifies the creation time of the backup image for which the table of contents is to be displayed. This parameter is optional. If you specify CREATIONTIME, you must also specify CREATIONDATE. If you do not specify these parameters, the contents of the latest backup image for the specified node and file space will be displayed, provided that this image has a table of contents. You can only specify the creation time as the following:

Value	Description	Example
HH:MM:SS	A specific time on the specified creation date.	10:30:08

This specifies that you want to display the contents of the backup image created on this time for the specified date. You can obtain this time from the output of the QUERY NASBACKUP command.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed for the files.

  Detailed
  : Specifies that complete information is displayed for the files, including the hexadecimal representation of each file or directory name.

Example: Display detailed table of contents information for a specific node

Use the QUERY TOC command to display information in the table of contents belonging to NAS node NETAPP in the file space /vol/vol1 created on 12/06/2002 at 11:22:46. Specify a detailed format.

```
query toc netapp /vol/vol1 creationdate=12/06/2002 creationtime=11:22:46
    format=detailed

Objects in the image backed up on 12/06/2002 11:22:46
for filespace /vol/vol1 in node NETAPP:


                                Object Name: /.etc
```

```
          Hexadecimal Object Name: 2f657463
                      Object Type: Directory
                      Object Size: 4,096
Last data Modification Date/Time: 07/31/2002 14:21:19

                      Object Name: /.etc/oldmaps/ndmp
          Hexadecimal Object Name: 2f6574632f6f6c646d6170
                                   732f6e646d70
                      Object Type: Directory
                      Object Size: 4,096
Last data Modification Date/Time: 07/31/2002 14:21:19

                      Object Name: /.etc/oldmaps/ndmp/TSM
                                  /vol/vol1/3df0e8fd
          Hexadecimal Object Name: 2f6574632f6f6c646d6170
                                   732f6e646d702f54534d2
                                   02f766f6c2f766f6c312f3
                                   364663065386664
                      Object Type: File
                      Object Size: 36,864
Last data Modification Date/Time: 12/06/2002 11:14:22
```

Field descriptions

Object Name
: The name of the object.

Hexadecimal Object Name
: The name of the object in hexadecimal format.

Object Type
: The type of the object.

Object Size
: The size of the object.

Last data Modification Date/Time
: The date and time the object was last modified.

Related commands

Table 1. Commands related to QUERY TOC

Command	Description
BACKUP NODE	Backs up a network-attached storage (NAS) node.
QUERY NASBACKUP	Displays information about NAS backup images.
RESTORE NODE	Restores a network-attached storage (NAS) node.

QUERY VIRTUALFSMAPPING (Query a virtual file space mapping)

Use this command to query a virtual file space mapping definition.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-Query VIRTUALFSmapping ------------------------------------>

   .-*--*---------------------------------.
>--+-------------------------------------+------------------><
   |            .-*----------------------. |
   '-node_name--+------------------------+-'
                '-virtual_filespace_name-'
```

Parameters

node_name
: Specifies the client node to which the virtual file space belongs. You can use wildcard characters to specify this name. This parameter is optional. The default is all client node names. You must specify a value for this parameter if you specify a virtual file space name.

virtual_file_space_name
: Specifies the name of the virtual file space mappings to be queried. You can use wildcard characters to specify this name. This parameter is optional. If a value is not specified, all virtual file space mappings are queried. Virtual file space mapping names are case sensitive. Use the QUERY VIRTUALFSMAPPING command to determine the correct capitalization for the virtual file space mapping to be queried.

Example: Display virtual file spaces for a specific node

Display the currently defined virtual file spaces for node NAS1. See Field descriptions for field descriptions.

```
query virtualfsmapping nas1

Node     Virtual Filespace  Filespace   Path              Hexadecimal
Name     Mapping Name       Name                          Path?
------   -----------------  ----------  ----------------- -----------
NAS1     /mikesdir          /vol/vol2   /mikes            No
NAS1     /tmpdir            /vol/vol1   /tmp              No
NAS1     /nonASCIIDir       /vol/vol3   2f73657276657231  Yes
```

Field descriptions

Node Name
: Specifies the name of the client node.

Virtual Filespace Mapping Name
: Specifies the name of the virtual file space mapping.

Filespace Name

: The name of the file space that belongs to the node.

: File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

: If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

Path
: Specifies the path to the client node.

Hexadecimal Path
: Indicates whether the path is hexadecimal.

Related commands

Table 1. Commands related to QUERY VIRTUALFSMAPPING

Command	Description
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
DELETE VIRTUALFSMAPPING	Delete a virtual file space mapping.
UPDATE VIRTUALFSMAPPING	Update a virtual file space mapping.

QUERY VOLHISTORY (Display sequential volume history information)

Use this command to display sequential volume history information. To save sequential volume history information to one or more files, use the BACKUP VOLHISTORY command.

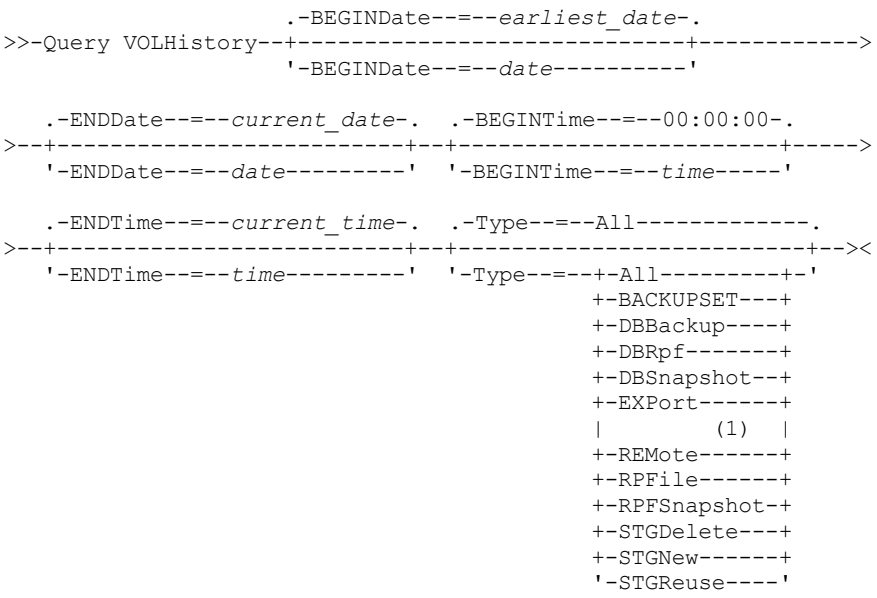
Use the VOLUMEHISTORY server option to specify one or more volume history files. After the server is restarted, IBM Spectrum Protect™ updates volume information in both the database and the files.

Use the QUERY BACKUPSET command to query specified backup set information.

Privilege class

Any administrator can issue this command.

Syntax



Notes:

1. This parameter is only available on AIX, HP-UX, Linux, Solaris and Windows operating systems.

Parameters

BEGINDate

Specifies that you want to display information beginning with records created on the specified date. This parameter is optional. The default is the earliest date for which history information exists.

You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified	TODAY–7 **or** –7. To display information beginning with records created a week ago, specify BEGINDATE=TODAY-7 or BEGINDATE=-7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.

Value	Description	Example
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDDate

Specifies that you want to display information ending with records created on the specified date. This parameter is optional. The default is the current date.

You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY-days **or** -days	The current date minus days specified. The maximum number of days is 9999.	TODAY–1 **or** –1. To display records created up to yesterday, specify ENDDATE=TODAY-1 or ENDDATE=-1.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies that you want to display information beginning with records created at the specified time. This parameter is optional. The default is midnight (00:00:00).

You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time on the specified begin date	12:33:28
NOW	The current time on the specified begin date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified begin date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 with BEGINTIME=NOW+03:00 or BEGINTIME=+03:00. IBM Spectrum Protect displays records with a time of 12:00 or later on the begin date.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-03:30 **or** -03:30. If you issue this command at 9:00 with BEGINTIME=NOW-03:30 or BEGINTIME=-03:30, IBM Spectrum Protect displays records with a time of 5:30 or later on the begin date.

ENDTime

Specifies that you want to display information ending with records created at the specified time on the end date. This parameter is optional. The default is the current time.

You can specify the time using one of the values below:

Value	Description	Example

Value	Description	Example
HH:MM:SS	A specific time on the specified end date	10:30:08
NOW	The current time on the specified end date	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes on the specified end date	NOW+03:00 **or** +03:00. If you issue this command at 9:00 with ENDTIME=NOW+03:00 or ENDTIME=+03:00, IBM Spectrum Protect displays records with a time of 12:00 or later on the end date.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified end date	NOW-03:30 **or** -03:30 If you issue this command at 9:00 with ENDTIME=NOW-3:30 or ENDTIME=-3:30, IBM Spectrum Protect displays records with a time of 5:30 or earlier on the end date.

Type

Specifies the type of records to display from the volume history file. This parameter is optional. The default is ALL. Possible values are:

All
: Specifies all records.

BACKUPSET
: Specifies to display only information about backup set volumes.

DBBackup
: Specifies to display only records that contain information about full and incremental database backup volumes, that is with the volume types of BACKUPFULL and BACKUPINCR.

DBRpf
: Specifies to display only records that contain information about full and incremental database backup volumes and recovery plan file object volumes (volume types of BACKUPFULL, BACKUPINCR, and RPFILE).

DBSnapshot
: Specifies to display only records that contain information about volumes used for database snapshot backups.

EXPort
: Specifies only records that contain information about export volumes.

REMote
: Specifies to display only records that contain information about volumes used by library clients.

RPFile
: Specifies to display only records that contain information about file objects of a recovery plan that are saved on a target server and that were created assuming database full and incremental backups. The parameter displays only records about recovery plan files that are saved on another IBM Spectrum Protect server by using the server-to-server virtual volume function for IBM Spectrum Protect.

RPFSnapshot
: Specifies to display only records that contain information about file objects of a recovery plan that are saved on a target server and that were created assuming database snapshot backups. RPFSnapshot only displays records about recovery plan files that are saved on another IBM Spectrum Protect server by using the server-to-server virtual volume function for IBM Spectrum Protect.

STGDelete
: Specifies only records that contain information about deleted sequential storage pool volumes.

STGNew
: Specifies only records that contain information about new sequential access storage volumes.

STGReuse
: Specifies only records that contain information about reused sequential storage pool volumes.

Example: Display volume history information for a storage pool volume

Display volume history information for a storage pool volume stored in the database. See Field descriptions for field descriptions. Issue the command:

```
query volhistory type=stgnew
```

```
                              Date/Time: 02/25/2011 18:28:06
                            Volume Type: STGNEW
                           Backup Series:
                        Backup Operation:
                              Volume Seq:
                            Device Class: FILE
                             Volume Name: /adsmfct/server/prvol1
                          Volume Location:
                                  Command:
                    Database Backup ID High:
                     Database Backup ID LOW:
              Database Backup Home Position:
                         Database Backup HLA:
                         Database Backup LLA:
      Database Backup Total Data Bytes (MB):
       Database Backup total Log Bytes (MB):
             Database Backup Block Num High:
              Database Backup Block Num Low:
                  Database Backup Stream Id:
Database Backup Volume Sequence for Stream:
```

Note: The volume history file will contain additional fields that do not appear in the query output. These fields are specific to database backup and restore support. They are not intended for use or modification by IBM Spectrum Protect administrators. The fields will be bracketed with a message indicating these are for IBM Spectrum Protect internal use only and not meant to be modified.

Example: Display volume history information for a database backup volume

Display volume history information for a database backup volume stored in the database. See Field descriptions for field descriptions. Issue the command:

```
query volhistory type=dbb
```

```
                              Date/Time: 02/25/2011 18:28:06
                            Volume Type: BACKUPFULL
                           Backup Series: 176
                        Backup Operation: 0
                              Volume Seq: 0
                            Device Class: FILE
                             Volume Name: /adsmfct/server/prvol1
                          Volume Location:
                                  Command:
                    Database Backup ID High: 0
                     Database Backup ID LOW: 0
              Database Backup Home Position: 0
                         Database Backup HLA:
                         Database Backup LLA:
      Database Backup Total Data Bytes (MB): 0
       Database Backup total Log Bytes (MB): 0
             Database Backup Block Num High: 0
              Database Backup Block Num Low: 0
                  Database Backup Stream Id: 1
Database Backup Volume Sequence for Stream: 10,001
```

Note: The volume history file will contain additional fields that do not appear in the query output. These fields are specific to database backup and restore support. They are not intended for use or modification by IBM Spectrum Protect administrators. The fields will be bracketed with a message indicating these are for IBM Spectrum Protect internal use only and not meant to be modified.

Field descriptions

Date/Time
: The date and time that the volume was created.

Volume Type
: The type of volume:

  BACKUPFULL
  : Full database backup volume.

BACKUPINCR
: Incremental database backup volume.

BACKUPSET
: Client backup set volume.

DBSNAPSHOT
: Snapshot database backup volume.

EXPORT
: Export volume.

REMOTE
: A volume used on the library client, which is the IBM Spectrum Protect server named in the Volume Location field. See the volume history on the server that is the library client to get details about how the volume is used.

RPFILE
: Recovery plan file object volume created assuming full and incremental database backups.

RPFSnapshot
: Recovery plan file object volume created assuming snapshot database backups.

STGDELETE
: Deleted sequential access storage pool volume.

STGNEW
: Added sequential access storage pool volume.

STGREUSE
: Reused sequential access storage pool volume.

Backup Series
: The value of this field depends on the volume type:

  - For BACKUPFULL or BACKUPINCR volume types: the backup series identifier.
  - For the DBSNAPSHOT volume type: the identifier of the backup series that is associated with the DBSNAPSHOT entry.
  - For the RPFILE volume type: the identifier of the backup series that is associated with the RPFILE entry.
  - For the RPFSNAPSHOT volume type: the identifier of the backup series that is associated with the RPFSNAPSHOT entry.
  - For BACKUPSET volume types: this field is blank.
  - For all other volume types: always 0.

  A backup series is a full backup and all incremental backups that apply to that full backup. Another series begins with the next full backup of the database.

Backup Operation
: For BACKUPFULL or BACKUPINCR volume types: the operation number of this backup volume within the backup series. The full backup within a backup series is operation 0. The first incremental backup for that full backup is operation 1, the second incremental backup is operation 2, and so on.

  For DBSNAPSHOT volume types: the operation number of this DBSNAPSHOT volume within the DBSNAPSHOT series.

  For all other volume types: always 0.

  This field is blank when the volume type is BACKUPSET.

Volume Seq
: The sequence or position of the volume within the backup series.

  - For BACKUPFULL or BACKUPINCR volume types: the sequence, or position, of the volume within the backup series. Volume sequence 1 identifies the first volume used for the first operation (a full backup), and so on. For example, if the full backup occupies three volumes, these volumes are identified as volume sequence 1, 2, and 3, respectively. The first volume of the next operation (the first incremental backup) is then volume sequence 4.
  - For BACKUPSET volume types: the sequence, or position, of the volume within the BACKUPSET series.
  - For DBSNAPSHOT volume types: the sequence, or position, of the volume within the DBSNAPSHOT series. Volume sequence 1 identifies the first volume used for the first DBSNAPSHOT operation, and so on.
  - For EXPORT volume types: the sequence number of the volume when it was used for exporting data.
  - For RPFILE volume types: the value of this field is always one (1).
  - For all other volume types: always 0.

Device Class
: The name of the device class associated with this volume.

Volume Name
: The name of the volume.

Volume Location
: The location of the volume. This information is available only for the following volume types:

  - BACKUPFULL
  - BACKUPINCR
  - EXPORT
  - REMOTE
  - RPFILE

  For the volume type of REMOTE, this location field is the server name of the library client that owns this volume.

  For the volume type of RPFILE, this location field is the server name defined in the device class definition used by the PREPARE command when the DEVCLASS parameter is specified.

Command
: When the volume type is EXPORT or BACKUPSET and the volume sequence is 1 (for example, the first volume), this field shows the command that was used to generate the volume. If the EXPORT or BACKUPSET is on more than one volume, the command is displayed with the first volume but not with any of the other volumes.

  For any volume type other than EXPORT or BACKUPSET, this field is blank.

Tip: The following fields are not used by IBM Spectrum Protect servers that are V6.3 or later. However, the fields are displayed for compatibility with earlier releases.

- Database Backup ID High
- Database Backup ID Low
- Database Backup Home Position
- Database Backup HLA
- Database Backup LLA
- Database Backup Total Data Bytes (MB)
- Database Backup Total Log Bytes (MB)
- Database Backup Block Num High
- Database Backup Block Num Low

Related commands

Table 1. Commands related to QUERY VOLHISTORY

Command	Description
BACKUP VOLHISTORY	Records volume history information in external files.
DELETE VOLHISTORY	Removes sequential volume history information from the volume history file.
PREPARE	Creates a recovery plan file.
QUERY RPFILE	Displays information about recovery plan files.
QUERY BACKUPSET	Displays backup sets.
UPDATE VOLHISTORY	Adds or changes location information for a volume in the volume history file.

QUERY VOLUME (Query storage pool volumes)

Use this command to display information about one or more storage pool volumes.

Privilege class

Any administrator can issue this command.

Syntax

Parameters

volume_name
: Specifies the volume to query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a name, all storage pool volumes are included in the query.

ACCess
: Specifies that output is restricted by volume access mode. This parameter is optional. You can specify multiple access modes by separating the modes with commas and no intervening spaces. If you do not specify a value for this parameter, output is not restricted by access mode. Possible values are:

  READWrite
  : Display volumes with an access mode of READWRITE. Client nodes and server processes can read from and write to files stored on the volumes.

  READOnly
  : Display volumes with an access mode of READONLY. Client nodes and server processes can read only files that are stored on the volumes.

  UNAVailable
  : Display volumes with an access mode of UNAVAILABLE. Client nodes and server processes cannot access files that are stored on the volumes.

  OFFsite
  : Display copy storage pool volumes with an access mode of OFFSITE. The volumes are at offsite locations from which they cannot be mounted.

  DEStroyed
  : Display primary storage pool volumes with an access mode of DESTROYED. The volumes are designated as permanently damaged.

STatus
: Specifies that output is restricted by volume status. This parameter is optional. You can specify multiple status values by separating values with commas and no intervening spaces. If you do not specify a value for this parameter, output is not restricted by volume status. Possible values are:

  ONline
  : Display random access volumes that are available to the server.

OFfline
: Display random access volumes that are not available to the server.

EMPty
: Display sequential access volumes that have no data.

PENding
: Display volumes with a status of PENDING. These volumes might be sequential-access volumes from which all files were deleted, but for which the time specified by the REUSEDELAY parameter on the DEFINE STGPOOL command has not elapsed. These volumes might also be random-access disk volumes that were deleted, but that still contain discarded data that is waiting to be shredded. After the data is shredded, the volume will be physically deleted.

FILling
: Display sequential access volumes that the server has written to but has not yet filled to capacity.

FULl
: Display sequential access volumes that the server filled.

STGPool
: Specifies the storage pool to include in the query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a storage pool name, all storage pools are included in the query.

DEVclass
: Specifies the device class to include in the query. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a device class name, all devices are included in the query.

Format
: Specifies how the information is displayed. This parameter is optional. The default value is STANDARD. Possible values are:

  Standard
  : Specifies that partial information is displayed.

  Detailed
  : Specifies that complete information is displayed.

AIX Linux

Example: List all file storage pool volumes

Display information on all storage pool volumes with the device class name of FILE. See Field descriptions for field descriptions.

```
query volume devclass=file
```

```
Volume Name              Storage     Device     Estimated  Pct   Volume
                         Pool Name   Class Name  Capacity  Util  Status
----------------------- ----------- ---------- --------- ----- -------
/FCT/SERVER/COVOl1       COPYSTG      FILE          0.0 M   0.0 Pending
/FCT/SERVER/COVOl2       COPYSTG      FILE          0.0 M   0.0 Empty
/FCT/SERVER/COVOl3       COPYSTG      FILE          0.0 M   0.0 Empty
/FCT/SERVER/PRVOl1       PRIMESTG     FILE          0.0 M   0.0 Empty
/FCT/SERVER/PRVOl2       PRIMESTG     FILE          0.0 M   0.0 Empty
```

Windows

Example: List all storage pool volumes with the same prefix

Display information on all storage pool volumes that are prefixed with the name ATF. See Field descriptions for field descriptions.

```
query volume atf*
```

```
Volume Name              Storage     Device     Estimated  Pct   Volume
                         Pool Name   Class Name  Capacity  Util  Status
----------------------- ----------- ---------- --------- ----- -------
ATF001                   8MMPOOL     8MMTAPE       4.8 G   18.2 Filling
ATF002                   8MMPOOL     8MMTAPE       4.8 G   18.2 Filling
```

AIX Linux

Example: Display detailed information about a specific storage pool volume

Display details about the storage pool volume named /fct/server/covol1. See Field descriptions for field descriptions.

```
query volume covol1 format=detailed
```

```
                    Volume Name: /FCT/SERVER/COVOl1
                Storage Pool Name: COPYSTG
                Device Class Name: DISK
              Estimated Capacity: 10.0 M
         Scaled Capacity Applied:
                        Pct Util: 6.7
                  Volume Status: On-line
                         Access: Read/Write
          Pct. Reclaimable Space: 3.2
                 Scratch Volume?: Yes
                 In Error State?: No
       Number of Writable Sides: 1
        Number of Times Mounted: 11
              Write Pass Number: 1
      Approx. Date Last Written: 04/14/1998 16:17:26
         Approx. Date Last Read: 04/01/1998 13:26:18
            Date Became Pending:
         Number of Write Errors: 0
          Number of Read Errors: 0
                Volume Location:
 Volume is MVS Lanfree Capable: No
Last Update by (administrator): COLLIN
          Last Update Date/Time: 05/01/1998 14:07:27
           Begin Reclaim Period:
             End Reclaim Period:
        Logical Block Protected:
  Drive Encryption Key Manager:
```

Windows

Example: Display detailed information about a specific storage pool volume

Display details about the storage pool volume WPDV00. See Field descriptions for field descriptions.

```
query volume wpdv00 format=detailed
```

```
                    Volume Name: WPDV00
                Storage Pool Name: TAPEPOOL
                Device Class Name: TAPE
              Estimated Capacity: 5.8 M
         Scaled Capacity Applied:
                        Pct Util: 0.1
                  Volume Status: On-line
                         Access: Read/Write
          Pct. Reclaimable Space: 3.2
                 Scratch Volume?: Yes
                 In Error State?: No
       Number of Writable Sides: 1
        Number of Times Mounted: 11
              Write Pass Number: 1
      Approx. Date Last Written: 04/14/1998 16:17:26
         Approx. Date Last Read: 04/01/1998 13:26:18
            Date Became Pending:
         Number of Write Errors: 0
          Number of Read Errors: 0
                Volume Location:
 Volume is MVS Lanfree Capable: No
Last Update by (administrator): COLLIN
          Last Update Date/Time: 05/01/1998 14:07:27
           Begin Reclaim Period:
             End Reclaim Period:
        Logical Block Protected:
  Drive Encryption Key Manager:
```

Example: Display detailed information about a storage pool volume with a specific device class

Display details about a volume in a storage pool with a device class name of FILECLASS. See Field descriptions for field descriptions.

```
query volume devclass=fileclass format=detailed
```

```
Windows Volume Name: Z:\WORM_CFS\0000000E.BFS
AIX Linux Volume Name: /WORM_FILESYS/0000000E.BFS
            Storage Pool Name: FILEPOOL
            Device Class Name: FILECLASS
          Estimated Capacity: 2.0 G
      Scaled Capacity Applied:
                    Pct Util: 0.0
                Volume Status: Filling
                      Access: Read/Write
       Pct. Reclaimable Space: 0.0
              Scratch Volume?: Yes
              In Error State?: No
     Number of Writable Sides: 1
      Number of Times Mounted: 1
            Write Pass Number: 1
    Approx. Date Last Written: 03/22/2004 15:23:46
       Approx. Date Last Read: 03/22/2004 15:23:46
          Date Became Pending:
       Number of Write Errors: 0
        Number of Read Errors: 0
              Volume Location:
 Volume is MVS Lanfree Capable: No
Last Update by (administrator):
         Last Update Date/Time: 03/22/2004 15:23:46
          Begin Reclaim Period: 03/22/2005
            End Reclaim Period: 04/22/2005
      Logical Block Protected:
  Drive Encryption Key Manager:
```

Example: Display detailed information about a specific storage pool volume

Display details about a storage pool volume that is named 000642. The volume is in a storage pool that is associated with a 3592 device class. See Field descriptions for field descriptions.

```
query volume 000642 format=detailed
```

```
                  Volume Name: 000642
            Storage Pool Name: 3592POOL
            Device Class Name: 3592CLASS
          Estimated Capacity: 2.0 G
      Scaled Capacity Applied:
                    Pct Util: 0.0
                Volume Status: Filling
                      Access: Read/Write
       Pct. Reclaimable Space: 0.0
              Scratch Volume?: Yes
              In Error State?: No
     Number of Writable Sides: 1
      Number of Times Mounted: 1
            Write Pass Number: 1
    Approx. Date Last Written: 03/22/2004 15:23:46
       Approx. Date Last Read: 03/22/2004 15:23:46
          Date Became Pending:
       Number of Write Errors: 0
        Number of Read Errors: 0
              Volume Location:
 Volume is MVS Lanfree Capable: No
Last Update by (administrator):
         Last Update Date/Time: 03/22/2004 15:23:46
          Begin Reclaim Period: 03/22/2005
            End Reclaim Period: 04/22/2005
      Logical Block Protected: Yes
  Drive Encryption Key Manager: IBM Spectrum Protect
```

Field descriptions

Volume Name
: The name of the storage pool volume.

Storage Pool Name
: The storage pool to which the volume is defined.

Device Class Name

The device class that is assigned to the storage pool.

Estimated Capacity
: The estimated capacity of the volume, in megabytes (M), gigabytes (G), or terabytes (T).

  For DISK devices, this value is the capacity of the volume.

  For sequential access devices, this value is an estimate of the total space available on the volume, which is based on the device class.

Scaled Capacity Applied
: The percentage of capacity to which a volume is scaled. For example, a value of 20 for a volume whose maximum capacity is 300 GB indicates that the volume can store only 20 percent of 300 GB, or 60 GB. This attribute applies only to IBM® 3592 devices.

Pct Util
: An estimate of the utilization of the volume. The utilization includes all space that is occupied by both files and aggregates, including empty space within aggregates.

  For DISK volumes, the utilization also includes space that is occupied by cached data.

Volume Status
: The status of the volume.

Access
: Whether the volume is available to the server.

Pct. Reclaimable Space (sequential access volumes only)
: The amount of space on this volume that can be reclaimed because data has expired or been deleted. This value is compared to the reclamation threshold for the storage pool to determine whether reclamation is necessary. Reclaimable space includes empty space within aggregates.

  When determining which volumes in a storage pool to reclaim, the server first determines the reclamation threshold. The reclamation threshold is indicated by the value of the THRESHOLD parameter on the RECLAIM STGPOOL command or, if that value was not specified, the value of the RECLAIM parameter in a storage pool definition. The server then examines the percentage of reclaimable space for each volume in the storage pool. If the percentage of reclaimable space on a volume is greater that the reclamation threshold of the storage pool, the volume is a candidate for reclamation.

  For example, suppose that storage pool FILEPOOL has a reclamation threshold of 70 percent. This value indicates that the server can reclaim any volume in the storage pool that has a percentage of reclaimable space that is greater that 70 percent. The storage pool has three volumes:

  - FILEVOL1 with 65 percent reclaimable space
  - FILEVOL2 with 80 percent reclaimable space
  - FILEVOL3 with 95 percent reclaimable space

  When reclamation begins, the server compares the percent of reclaimable space for each volume with the reclamation threshold of 70 percent. In this example, FILEVOL2 and FILEVOL3 are candidates for reclamation because their percentages of reclaimable space are greater than 70.

  For volumes that belong to a SnapLock storage pool, the value is displayed but is not used.

Scratch Volume? (sequential access volumes only)
: Whether this volume is returned to scratch when the volume becomes empty.

In Error State?
: Whether the volume is in an error state. The server cannot write to volumes in an error state.

Number of Writable Sides
: This information is reserved for IBM Spectrum Protect™.

Number of Times Mounted
: The number of times that the server opened the volume for use. The number of times that the server opened the volume is not always the same as the number of times that the volume was physically mounted in a drive. After a volume is physically mounted, the server can open the same volume multiple times for different operations, for example for different client backup sessions.

Write Pass Number (sequential access volumes only)
: The number of times the volume was written to from the beginning to the end.

Approx. Date Last Written
: The approximate date on which the volume was last written.

Approx. Date Last Read
: The approximate date on which the volume was last read.

Date Became Pending
: The date that the status of the volume was changed to pending.

Number of Write Errors
: The number of writing errors that occurred on the volume.

Number of Read Errors
: The number of reading errors that occurred on the volume.

Volume Location
: The location of the volume.

Volume is MVS Lanfree Capable
: Whether the volume is LAN-free capable. A LAN-free capable volume is one that was defined and used (at least once) by the IBM Spectrum Protect z/OS® data manager server.

Last Update by (administrator)
: The administrator that defined or most recently updated the volume.

Last Update Date/Time
: When the volume was defined or most recently updated.

Begin Reclaim Period
: Represents the date after which the server begins reclaiming this volume, but not later than the date represented by the end reclaim period. If, when the reclaim period begins, there are files on the volume that have not expired, they are moved to a new WORM volume during reclamation processing. This field displays a date only if this volume is in a storage pool for which the value of the RECLAMATIONTYPE parameter is SNAPLOCK.

  If more than one archive is stored on the same volume, the start of the volume's reclamation period is based on the date of the most recent archive. For SnapLock volumes, the RETVer parameter of the DEFINE COPYGROUP command determines how long an archive is stored. If RETVer is set to 100 days, the volume's reclamation period will start 100 days after the first archive is stored on it. If a second archive is stored on the same volume, the reclamation start date will be adjusted to 100 days after the new archive is stored. If the RETVer value is changed after the first archive is stored, the latest reclamation date will apply for all of the archives on the volume. For example, assume RETVer is set to 100 for an initial archive, but is then changed to 50. If a second archive is stored on the volume three days after the first, the reclamation period will not start until 100 days after the first archive was stored.

End Reclaim Period
: Represents the date by which the IBM Spectrum Protect must complete reclamation processing on this volume to ensure continued protection of the data. It also represents the Last Access Date physical file attribute in the NetApp Filer, which prevents the file from being deleted until after that date. This field displays a date only if this volume is in a storage pool for which the value of the RECLAMATIONTYPE parameter is SNAPLOCK.

Drive Encryption Key Manager
: The drive encryption key manager. This field applies only to volumes in a storage pool that is associated with a device type of 3592, LTO, or ECARTRIDGE.

Logical Block Protected
: Specifies whether logical block protection is enabled for the volume. You can use logical block protection only with the following types of drives and media:

  - IBM LTO5 and later
  - IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later
  - Oracle StorageTek T10000C and T10000D drives

Related commands

Table 1. Commands related to QUERY VOLUME

Command	Description
DEFINE DEVCLASS	Defines a device class.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE VOLUME	Deletes a volume from a storage pool.
UPDATE DEVCLASS	Changes the attributes of a device class.
UPDATE VOLUME	Updates the attributes of storage pool volumes.
VARY	Specifies whether a disk volume is available to the server for use.

QUIT (End the interactive mode of the administrative client)

Use this command to end an administrative client session in interactive mode.

You cannot use the QUIT command from the SERVER_CONSOLE administrative ID, or the console, batch, or mount modes of the administrative client.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-QUIT-------------------------------------------------------><
```

Parameters

None.

Example: End an interactive administrative client session

End an administrative client session in the interactive mode.

```
quit
```

Related commands

None.

RECLAIM STGPOOL (Reclaim volumes in a sequential-access storage pool)

Use this command to reclaim volumes in a sequential-access storage pool. Reclamation does not move inactive versions of backup data from volumes in active-data pools.

This command cannot be used for the following types of storage pools:

- Container-copy storage pools. Space in these storage pools is reclaimed as part of the processing that is done by PROTECT STGPOOL commands.
- Storage pools with one of the following data formats:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Storage pools that use a CENTERA device class.
- Storage pools that use a Write Once Read Many (WORM) device class. Reclamation is not necessary because WORM volumes are not reusable, but you can run reclamation to consolidate data onto fewer volumes.

Use this command only if you are not going to use automatic reclamation for the storage pool. This command accepts the values of the RECLAIMPROCESS and RECLAIMSTGPOOL attributes of the storage pool definition. This command also accepts the values of the OFFSITERECLAIMLIMIT and RECLAIM parameters of the storage pool definition, if not overridden by the OFFSITERECLAIMLIMIT and THRESHOLD command parameters.

Tips:

- When you issue this command, duplicate data in a primary storage pool, copy storage pool, or active-data pool that is set up for data deduplication is removed.
- When you use this command to restore deduplicated objects to the same storage pool, any duplicate data blocks are replaced with references to deduplicated extents.

For storage pools defined with RECLAMATIONTYPE=SNAPLOCK, this command also deletes empty WORM FILE volumes that exceeded their reclaim period.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool that is being reclaimed and the reclaim storage pool, if applicable.

Syntax

```
>>-RECLaim STGpool--pool_name--+----------------------+--------->
                               '-THreshold--=--number-'

                             .-Wait--=--No------.
>--+----------------------+--+------------------+--------------->
   '-DUration--=--minutes-'  '-Wait--=--+-No--+-'
                                        '-Yes-'

>--+-------------------------------------------+--------------><
   '-OFFSITERECLAIMLimit--=--number_of_volumes-'
```

Parameters

pool_name (Required)
: Specifies the storage pool in which volumes are to be reclaimed.

DUration
: Specifies the maximum number of minutes that the reclamation runs before it is automatically canceled. You can specify a number 1 - 9999. This parameter is optional.

  After the specified number of minutes elapses, the next time the server checks the reclamation process the server stops the reclamation process. The server checks the reclamation process when the server mounts another eligible volume from the storage pool that is being reclaimed. The server also checks the reclamation process when the server begins to reclaim a new batch of files from the currently mounted volume. As a result, the reclamation can run longer than the value you specified for this parameter.

  Until the server checks the reclamation process, there is no indication the duration period expired. When the server stops the reclamation process, the server issues message ANR4927W: `Reclamation terminated for volume xxx - duration exceeded.`

  If you do not specify this parameter, the process stops only when no more volumes meet the threshold.

  If you specify a duration value for reclamation of a copy storage pool with offsite volumes, you might cause the reclamation to end before any volumes are reclaimed. In most situations when you initiate reclamation for a copy storage pool with offsite volumes, consider limiting the number of offsite volumes to be reclaimed rather than limiting the duration. For details, see the OFFSITERECLAIMLIMIT parameter.

THreshold
: Specifies the percentage of reclaimable space on a volume that makes it eligible for reclamation. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the server database. Reclaimable space also includes unused space.

  You can specify a number 1 - 99. This parameter is optional. If not specified, the RECLAIM attribute of the storage pool definition is used.

  To determine the percentage of reclaimable space for a volume, issue the QUERY VOLUME command and specify FORMAT=DETAILED. The value in the field Pct. Reclaimable Space is the percentage of reclaimable space for the volume.

  Specify a value of 50 percent or greater for this parameter so that files stored on two volumes can be combined into a single target volume.

OFFSITERECLAIMLimit
: Specifies the maximum number of offsite storage pool volumes that the server tries to reclaim. This parameter is valid only for copy storage pools. You can specify a number 0 - 99999. This parameter is optional. If not specified, the OFFSITERECLAIMLIMIT attribute of the storage pool definition is used.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. You can specify one of the following values:

No

Specifies that the server processes this command in the background.

You can continue with other tasks while the command is processed. Messages that are created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

If you cancel this process, some files might already be moved to new volumes before the cancellation.

Yes

Specifies that the server processes this command in the foreground. The operation must complete before you can continue with other tasks. Output messages are displayed to the administrative client when the operation completes. Messages are also displayed either in the activity log or the server console, or both, depending on where the messages are logged.
Restriction: You cannot specify WAIT=YES from the server console.

Example: Reclaim volumes in a sequential-access storage pool

Reclaim volumes in the storage pool named TAPEPOOL. Specify that reclamation ends as soon as possible after 60 minutes.

```
reclaim stgpool tapepool duration=60
```

Related commands

Table 1. Commands related to RECLAIM STGPOOL

Command	Description
CANCEL PROCESS	Cancels a background server process.
MIGRATE STGPOOL	Migrates files from a primary storage pool to the next storage pool in the hierarchy.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY PROCESS	Displays information about background processes.
QUERY STGPOOL	Displays information about storage pools.

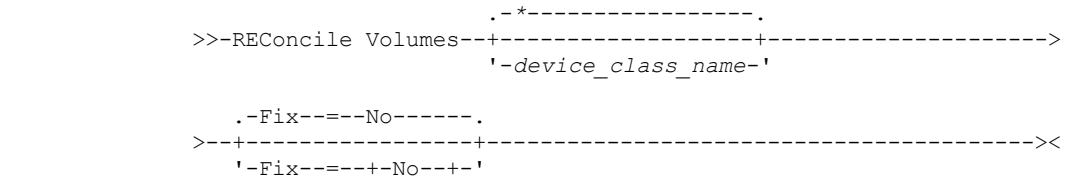
RECONCILE VOLUMES (Reconcile differences in the virtual volume definitions)

Issue this command from the source server to reconcile differences between virtual volume definitions on the source server and archive files on the target server. IBM Spectrum Protect™ finds all volumes of the specified device class on the source server and all corresponding archive files on the target server. The target server inventory is also compared to the local definition for virtual volumes to see if inconsistencies exist.

Privilege class

To issue this command, you must have system privilege.

Syntax



```
'-Yes-'
```

Parameters

device_class_name
: Specifies the device class name of the virtual volumes. If you do not specify a name, IBM Spectrum Protect reconciles all virtual volumes. This parameter is optional.

FIX
: Specifies whether or not IBM Spectrum Protect attempts to correct any identified inconsistencies. This parameter is optional. The default is NO. Possible values are:

  No
  : Specifies that IBM Spectrum Protect does not fix any inconsistencies.

  Yes
  : Specifies that IBM Spectrum Protect makes the following corrections:

    - IBM Spectrum Protect marks as unavailable storage pool volumes on the source server that cannot be located on the target server. Volumes that are only found in the volume history, such as database backups and import and export volumes, are reported as being inconsistent.
    - Archive files on the target server that do not correspond to any virtual volumes on the source server are marked for deletion from the target server.

    The following table shows the details of the actions taken:

FIX=	At the Source Server	At the Target Server	Action
NO	Volumes exist	No files exist	Report error
		Files exist but are marked for deletion	
		Active files exist but attributes do not match	
	Volumes do not exist	Active files exist	Report error
		Files exist but are marked for deletion	None
YES	Volumes exist	No files exist	Report error **Storage pool volumes:** Marked as unavailable
		Files exist but marked for deletion	Report error **Storage pool volumes:** If attributes match, mark files on the target server as active again, mark volumes on the source server as unavailable, and recommend that an AUDIT VOLUME be done to verify the data. If attributes do not match, mark volumes as unavailable.
		Active files exist but attributes do not match	Report error **Storage pool volumes:** Mark as unavailable and recommend that an AUDIT VOLUME be done to verify the data.
	Volumes do not exist	Active files exist	Mark files for deletion on the target server.
		Files exist but marked for deletion	None

Example: Reconcile differences in the virtual volume definitions

Reconcile the differences between all virtual volumes definitions on the source server and archive files on the target server to correct any inconsistencies.

```
reconcile volumes remote1 fix=yes
```

Related commands

Table 1. Commands related to RECONCILE VOLUMES

Command	Description
DEFINE DEVCLASS	Defines a device class.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE SERVER	Deletes the definition of a server.
QUERY SERVER	Displays information about servers.
UPDATE SERVER	Updates information about a server.

REGISTER commands

Use the REGISTER commands to define or add objects to IBM Spectrum Protect™.

- REGISTER ADMIN (Register an administrator ID)
- REGISTER LICENSE (Register a new license)
- REGISTER NODE (Register a node)

REGISTER ADMIN (Register an administrator ID)

Use this command to add an administrator to the server. After registration, the administrator can issue a limited set of commands, including all query commands. To provide additional privileges, use the GRANT AUTHORITY command.

Privilege class

To issue this command, you must have system privilege.

When you register an administrator with the same name as an existing node, be aware of the administrator authentication method and the SSLREQUIRED setting. Any node that has the same name as the administrator that is being registered inherits those settings.
For users of Lightweight Directory Access Protocol (LDAP) servers:

- The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
- Do not specify an administrative user ID that matches a node name. If the administrative user ID matches the node name, you might see unexpected behavior because of automatic password changes that update the same password twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update operation might fail.

Syntax

```
>>-REGister Admin--admin_name--+----------+--------------------->
                               '-password-'

>--+-----------------------+--+-----------------+------------->
   |  (1)                  |  '-CONtact--=--text-'
   '-------PASSExp--=--days-'

   .-FORCEPwreset--=--No------.
>--+--------------------------+-------------------------------->
   '-FORCEPwreset--=--+-No--+-'
                      '-Yes-'

>--+-----------------------------+---------------------------->
   '-EMAILADdress--=--userID@node-'

      (2)
```

```
   .-------AUTHentication--=--LOcal-.
>--+-------------------------------+--------------------------->
   '-AUTHentication--=--+-LOcal-+---'
                        '-LDap--'

                                (3)
   .-SSLrequired--=--DEFault-------.
>--+-----------------------------+--------------------------->
   '-SSLrequired--=--+-Yes-----+---'
                     +-No------+
                     '-DEFault-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+--------------------------------------+--------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-ALert--=--No------.
>--+-------------------+-------------------------------------><
   '-ALert--=--+-Yes-+-'
               '-No--'
```

Notes:

1. The PASSEXP command does not apply to administrators who authenticate to an LDAP directory server.
2. The default value can change if you issued the SET DEFAULTAUTHENTICATION command and specified LDAP.
3. The SSLREQUIRED parameter is deprecated.

Parameters

admin_name (Required)
: Specifies the name of the administrator to be registered. The maximum length of the name is 64 characters.

  You cannot specify an administrator name of NONE.

  If you plan to authenticate the administrator ID with an LDAP server, ensure that the administrator ID does not match the name of any node that authenticates with an LDAP server.

password
: Specifies the password of the administrator to be registered. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.
  If you authenticate passwords locally with the IBM Spectrum Protect server, you must specify a password. The password is not case-sensitive.
  If you authenticate passwords with a Lightweight Directory Access Protocol (LDAP) server, do not specify a password on the REGISTER ADMIN command.

PASSExp
: Specifies the number of days the password remains valid. You can set the password expiration period in the range 0 - 9999 days. A value of 0 means that the password never expires. This parameter is optional. If you do not specify this parameter, the password is set with the global expiration period of 90 days. This parameter does not affect passwords that authenticate with an LDAP directory server.

CONtact
: Specifies information identifying the administrator being registered. This parameter is optional. The maximum length of this string is 255 characters. The contact information must be enclosed in quotation marks if it contains any blanks.

FORCEPwreset
: Specifies whether the administrator is required to change or reset the password. This parameter is optional. The default value is NO. Possible values are:

  No
  : Specifies that the administrator does not need to change or reset the password while attempting to sign on to the server.

  Yes
  : Specifies that the administrator's password expires at the next sign-on. The client or administrator must change or reset the password then. If a password is not specified, you receive an error message.
    Restriction: For administrative user IDs that authenticate with an LDAP server, password expiration is set by using LDAP server utilities. For this reason, do not specify FORCEPWRESET=YES if you specify AUTHENTICATION=LDAP.

EMAILADdress
Specifies the email address for this administrator.

AUTHentication
This parameter specifies the authentication method for the administrator user ID. Specify one of the following values: LDAP or LOCAL. The parameter is optional and defaults to LOCAL. The default can change to LDAP if you use the SET DEFAULTAUTHENTICATION command and specify LDAP.

LOcal
Specifies that the local IBM Spectrum Protect server database is used.

LDap
Specifies that the administrator user ID authenticates passwords with an LDAP directory server. Passwords that authenticate with an LDAP directory server are case-sensitive.
Tip: A password is not required if you register an administrator and select `AUTHENTICATION=LDAP`. At logon, you are prompted for a password.

SSLrequired (deprecated)

Specifies whether the administrator user ID must use the Secure Sockets Layer (SSL) protocol to communicate between the IBM Spectrum Protect server and the backup-archive client. When you authenticate passwords with an LDAP directory server, you must protect the sessions by using SSL or another network security method.

Important: Beginning with IBM Spectrum Protect Version 8.1.2 software and Tivoli® Storage Manager Version 7.1.8 software, this parameter is deprecated. Validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The SSLREQUIRED parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

SESSIONSECurity
Specifies whether the administrator must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

You can specify one of the following values:

STRict
Specifies that the strictest security settings are enforced for the administrator. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the server and the administrator. To specify whether the server uses TLS 1.2 for the entire session or only for authentication, see the SSL client option.
To use the STRICT value, the following requirements must be met to ensure that the administrator can authenticate with the server:

- Both the administrator and server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
- The administrator must be configured to use the TLS 1.2 protocol for SSL sessions between the server and the administrator.

Administrators set to STRICT that do not meet these requirements are unable to authenticate with the server.

TRANSitional
Specifies that the existing security settings are enforced for the administrator. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the administrator has never met the requirements for the STRICT value, the administrator will continue to authenticate by using the TRANSITIONAL value. However, after an administrator meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the administrator can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after an administrator successfully authenticates by using a more secure communication protocol, the administrator can no longer authenticate by using a less secure protocol. For example, if an administrator that is not using SSL is updated and successfully authenticates by using TLS 1.2, the administrator can no longer authenticate by using no SSL protocol or TLS 1.1. This restriction also applies when you use functions such as command routing or server-to-server export, when the administrator authenticates to the IBM Spectrum Protect server as an administrator from another server.

ALert
Specifies whether alerts are sent to an administrators email address.

Yes

Specifies that alerts are sent to the specified administrators email address.

No

Specifies that alerts are not sent to the specified administrators email address. This is the default value.

Tip: Alert monitoring must be enabled, and email settings must be correctly defined to successfully receive alerts by email. To view the current settings, issue the QUERY MONITORSETTINGS command.

Example: Register an administrator

Define an administrator, LARRY, with the password PASSWORDONE. You can identify LARRY as second-shift personnel by specifying this information with the CONTACT parameter. Issue the command:

```
register admin larry passwordone contact='second shift'
```

Example: Register an administrator ID and set the authentication method

Define an administrator ID for Harry so that Harry can authenticate to an LDAP server. Issue the command:

```
register admin harry authentication=ldap
```

Example: Register an administrator and enforce strict session security

Register an administrator named Harry, and require Harry to use the strictest security settings to authenticate with the server. Issue the command:

```
register admin harry sessionsecurity=strict
```

Related commands

Table 1. Commands related to REGISTER ADMIN

Command	Description
GRANT AUTHORITY	Assigns privilege classes to an administrator.
LOCK ADMIN	Prevents an administrator from accessing IBM Spectrum Protect.
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE ADMIN	Removes an administrator from the list of registered administrators.
RENAME ADMIN	Changes an IBM Spectrum Protect administrator's name.
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
UNLOCK ADMIN	Enables a locked administrator to access IBM Spectrum Protect.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.
UPDATE NODE	Changes the attributes that are associated with a client node.

Related tasks:
Naming Tivoli Storage Manager objects
Related reference:
Ssl client option

REGISTER LICENSE (Register a new license)

Use this command to register new licenses for server components, including IBM Spectrum Protect™ (base), IBM Spectrum Protect Extended Edition, and IBM Spectrum Protect for Data Retention.

Licenses are stored in enrollment certificate files. The enrollment certificate files contain licensing information for the server product. The NODELOCK file preserves the licensing information for your installation. Your license agreement determines what you are licensed to use, even if you cannot use the REGISTER LICENSE command to register all components. You are expected to comply with the license agreement and use only what you have purchased. Use of the REGISTER LICENSE command implies that you agree to and accept the license terms specified in your license agreement.

Important:

- Before upgrading from a previous version of IBM Spectrum Protect, you must delete or rename the NODELOCK file.
- To unregister licenses, you must erase the NODELOCK file in the server instance directory of your installation, and reregister any previously registered licenses.
- You cannot register licenses for IBM Spectrum Protect for Mail, IBM Spectrum Protect for Databases, IBM Spectrum Protect for ERP, and IBM Spectrum Protect for Space Management.

To generate a report that can help you understand the license requirements for your system, run the QUERY PVUESTIMATE command. The report contains estimates of the number of client devices and PVU totals for server devices. The estimates are not legally binding.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-REGister LICense--FILE--=--+-tsmbasic.lic-+-----------------><
                              +-tsmee.lic-----+
                              +-dataret.lic--+
                              '-*.lic--------'
```

Parameters

FILE
: Specifies the name of the enrollment certificate file containing the license to be registered. The specification can contain a wildcard (*). Enter the complete file name or a wildcard in place of the file name. The file names are case-sensitive. The following values can be used:

  tsmbasic.lic
  : To license base IBM Spectrum Protect.

  tsmee.lic
  : To license IBM Spectrum Protect Extended Edition. This includes the disaster recovery manager, large libraries, and NDMP.

  dataret.lic
  : To license IBM Spectrum Protect for Data Retention. This is required to enable Data Retention Protection as well as Expiration and Deletion Suspension (Deletion Hold).

  *.lic
  : To license all IBM Spectrum Protect licenses for server components.

Example: Register a license

Register the base IBM Spectrum Protect license.

```
register license file=tsmbasic.lic
```

Related commands

Table 1. Commands related to REGISTER LICENSE

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.
QUERY LICENSE	Displays information about licenses and audits.
QUERY PVUESTIMATE	Displays processor value unit estimates.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET LICENSEAUDITPERIOD	Specifies the number of days between automatic license audits.

REGISTER NODE (Register a node)

Use this command to register a node to the server.

This command can create an administrative user ID with client owner authority over the node. You can use this administrative user ID to access the web backup-archive client from remote locations through a web browser.
Tip:

- In earlier product releases, the REGISTER NODE command automatically created an administrative user ID whose name matched the node name. Beginning with IBM Spectrum Protect™ V8.1, the REGISTER NODE command does not automatically create an administrative user ID that matches the node name.
- If you plan to use the LAN-free option with this node, you must register an administrative ID that matches the node name. To register the administrative ID, use the USERID parameter or manually register the administrator and grant owner authority to the node.

If a client requires a different policy domain than STANDARD, you must register the client node with this command or update the registered node.

Requirement: When you set `sslrequired=serveronly` in a REGISTER NODE command, the admin SSLREQUIRED setting reverts to YES. To use a non-SSL session with a storage agent, rename the admin with the identical name by issuing the RENAME ADMIN command.
For users of Lightweight Directory Access Protocol (LDAP) servers: The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
When you register or update a node, you can specify whether damaged files on the node can be recovered from a replication server. Files can be recovered only if all the following conditions are met:

- Version 7.1.1 or later, is installed on the source and target replication servers.
- The REPLRECOVERDAMAGED system parameter is set to ON. The system parameter can be set by using the SET REPLRECOVERDAMAGED command.
- The source server includes at least one file that is marked as damaged in the node that is being replicated.
- The node data was replicated before the damage occurred.

The following table describes how parameter settings affect the recovery of damaged, replicated files.

Table 1. Settings that affect the recovery of damaged files

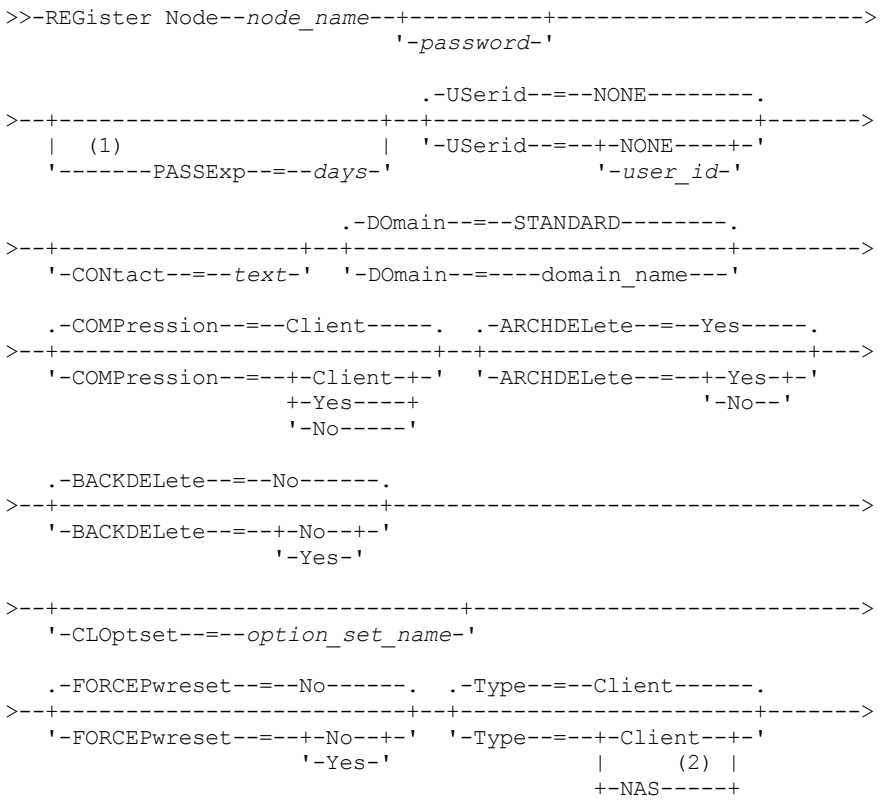
Setting for the REPLRECOVERDAMAGED system parameter	Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command	Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands	Result
OFF	YES, NO, or not specified	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
OFF	ONLY	YES or NO	An error message is displayed because files cannot be recovered when the REPLRECOVERDAMAGED system parameter is set to OFF.

Setting for the REPLRECOVERDAMAGED system parameter	Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command	Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands	Result
ON	YES	YES or NO	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	NO	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
ON	ONLY	YES or NO	Damaged files are recovered from the target replication server, but standard node replication does not occur.
ON	Not specified	YES	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	Not specified	NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.

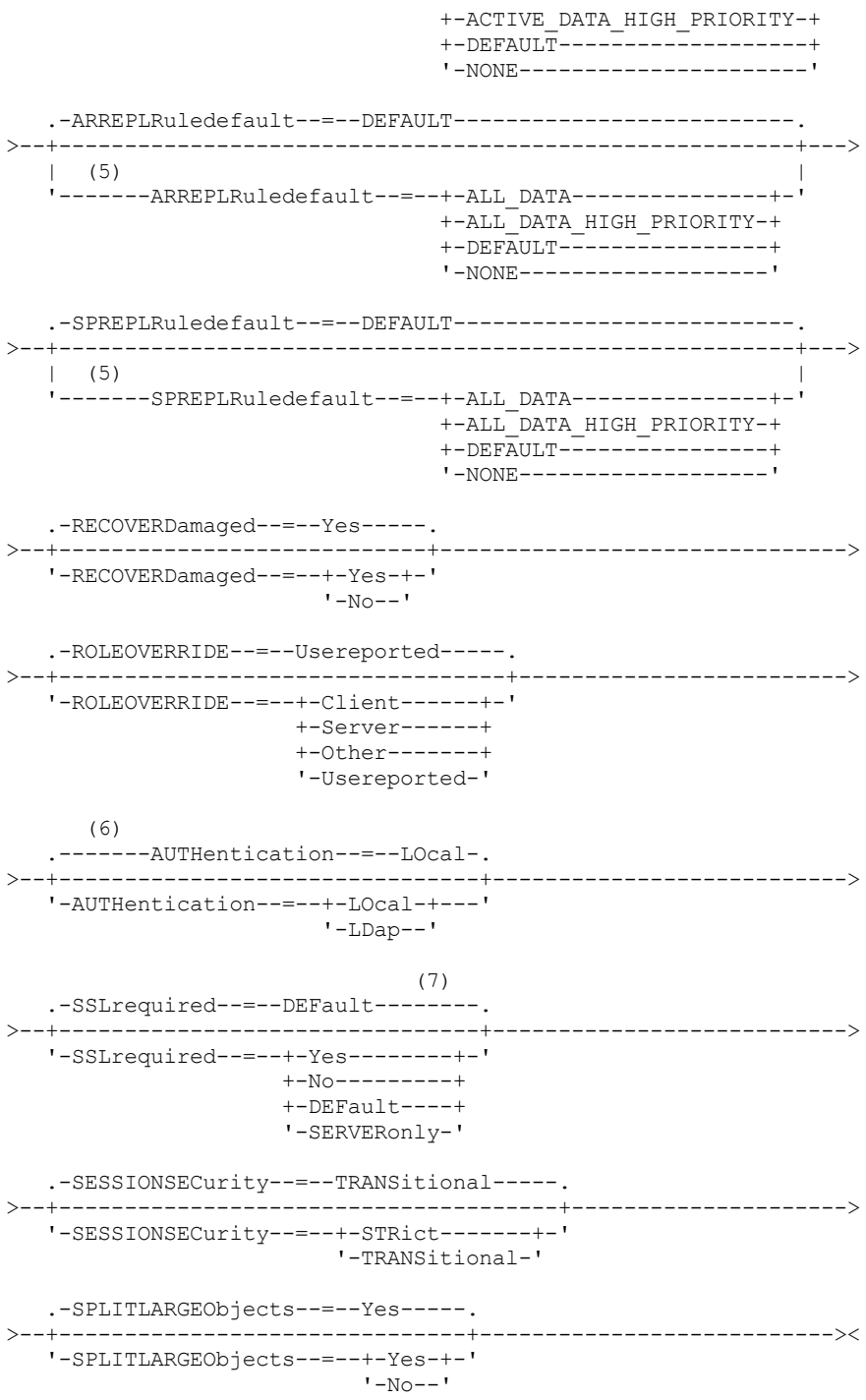
Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax




'-Server--'
'-URL--=--url-' '-UTILITYUrl--=--utility_url-'
.-MAXNUMMP--=--1------. .-AUTOFSRename--=--No---------.
'-MAXNUMMP--=--number-' '-AUTOFSRename--=--+-Yes----+-'
+-No-----+
'-Client-'
.-KEEPMP--=--No------. (3)
'-KEEPMP--=--+-No--+-'
'-Yes-'
.-VALIdateprotocol--=--No-----------.
'-VALIdateprotocol--=--+-No-------+-'
+-Dataonly-+
'-All------'
.-TXNGroupmax--=--0----------.
'-TXNGroupmax--=--+-0------+-'
'-number-'
.-DATAWritepath--=--ANY---------.
'-DATAWritepath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
.-DATAReadpath--=--ANY---------.
'-DATAReadpath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
'-TARGETLevel--=--V.R.M.F-'
.-SESSIONINITiation--=--Clientorserver---.
'-SESSIONINITiation--=--+-Clientorserver---+-'
'-SERVEROnly--HLAddress--=--ip_address--LLAddress--=--tcp_port-'
'-HLAddress--=--ip_address--LLAddress--=--tcp_port-'
'-EMAILADdress--=--userID@node-'
.-DEDUPlication--=--Clientorserver-----.
'-DEDUPlication--=--+-Clientorserver-+-'
'-SERVEROnly-----'
.-BACKUPINITiation--=--All----------.
| (4) |
'-BACKUPINITiation--=--+-All--+-----'
'-ROOT-'
'-REPLState--=--+-ENabled--+-'
'-DISabled-'
.-BKREPLRuledefault--=--DEFAULT----------------------------.
| (5) |
'-------BKREPLRuledefault--=--+-ALL_DATA-----------------+-'
+-ACTIVE_DATA---------------+
+-ALL_DATA_HIGH_PRIORITY----+



Notes:

1. The PASSEXP command does not apply to administrators who authenticate with a Lightweight Directory Access Protocol (LDAP) directory server.
2. This parameter is only available for AIX®, Linux, and Windows operating systems.
3. The VALIDATEPROTOCOL parameter is deprecated.
4. The BACKUPINITIATION parameter is ignored if the client node operating system is not supported.
5. You can specify the BKREPLRULEDEFAULT, ARREPLRULEDEFAULT, or SPREPLRULEDEFAULT parameter only if you specify the REPLSTATE parameter.
6. The default value can change if you issued the SET DEFAULTAUTHENTICATION command and specified LDAP.
7. The SSLREQUIRED parameter is deprecated.

Parameters

node_name (Required)
Specifies the name of the client node to be registered. The maximum length of the name is 64 characters.

You cannot specify a node name of NONE.

password
Specifies the client node password. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

If you authenticate passwords locally with the IBM Spectrum Protect server, you must specify a password. The password is not case-sensitive.

If you authenticate passwords with an LDAP server, do not specify a password on the REGISTER NODE command.

PASSExp
Specifies the number of days the password remains valid. You can set the password expiration period 0 - 9999 days. A value of 0 means that the password never expires. This parameter is optional. If you do not specify this parameter, the server common-password expiration period is used. The common password expiration period is 90 days unless changed by issuing the SET PASSEXP command.

You can change the password expiration period by using the UPDATE NODE or SET PASSEXP commands. You can issue the SET PASSEXP command to set a common expiration period for all administrators and client nodes. You can also use the command to selectively set password expiration periods. If you selectively set a password expiration period by using the REGISTER NODE command, the UPDATE NODE command, or the SET PASSEXP command, the expiration period is excluded from common password expiration periods that were created by using the SET PASSEXP command.

You can use the RESET PASSEXP command to reset the password expiration period to the common expiration period. The PASSEXP command does not apply to nodes that authenticate with an LDAP server.

USerid
Specifies the administrative user ID with client owner authority. This parameter is optional. You can specify one of the following values:

NONE
Specifies that no administrative user ID is created. This is the default value.

user_id
Specifies that an administrative user ID is created with the specified name. You can use this parameter to grant client owner authority to an existing administrative user ID.

If you register a node that has the same name as an administrator, the administrator authentication method and SSLREQUIRED setting change to match the authentication method of the node. Passwords that are shared between same-named nodes and administrators are kept synchronized during an authentication change.

If you plan to use the LAN-free option with this node, use the USERID parameter to register an administrative ID that matches the node name.

For users of LDAP servers: If you plan to authenticate the node with an LDAP server, keep the default setting (USERID=NONE) or specify an administrative user ID that differs from the node name. If the administrative user ID matches the node name, you might see unexpected behavior because of automatic password changes that update the same password twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update operation might fail.

CONtact
Specifies a text string of information that identifies the node. The parameter is optional. The maximum length of the text string is 255 characters. The contact information must be enclosed in quotation marks if it contains any blanks.

DOmain
Specifies the name of the policy domain to which the node is assigned. The parameter is optional. If you do not specify a policy domain name, the node is assigned to the default policy domain (STANDARD).

When a source server is registered as a node, it is assigned to a policy domain. Data from the source server is stored in the storage pool that is specified in the archive copy group of the default management class of that domain.

COMPression
Specifies whether the client node compresses its files before it sends these files to the server for backup and archive. The parameter is optional. The default value is CLIENT.
Restriction: This parameter does not apply to nodes with a type of NAS or SERVER.

You can specify one of the following values:

Client
: Specifies that the client determines whether to compress files.

Yes
: Specifies that the client node compresses its files before it sends these files to the server for backup and archive.

No
: Specifies that the client node does not compress its files before it sends these files to the server for backup and archive.

ARCHDELete
: Specifies whether the client node can delete its own archive files from the server. The parameter is optional. The default value is YES. You can specify one of the following values:

Yes
: Specifies that the client node can delete its own archive files from the server.

No
: Specifies that the client node cannot delete its own archive files from the server.

BACKDELete
: Specifies whether the client node can delete its own backup files from the server. The parameter is optional. The default value is NO. You can specify one of the following values:

No
: Specifies that the client node cannot delete its own backup files from the server.

Yes
: Specifies that the client node can delete its own backup files from the server.

CLOptset
: Specifies the name of the option set to be used by the client. The parameter is optional.

FORCEPwreset
: Specifies whether to force a client to change or reset the password. The parameter is optional. The default value is NO. You can specify one of the following values:

No
: Specifies that the password expiration period is set by the SET PASSEXP command. The client does not need to change or reset the password while the client is logging on to the server.

Yes
: Specifies that the client node password expires at the next logon. The client must change or reset the password then. If a password is not specified, you receive an error message.
Restriction: For nodes that authenticate with an LDAP server, password expiration is set by using LDAP server utilities. For this reason, do not specify FORCEPWRESET=YES if you specify AUTHENTICATION=LDAP.

Type
: Specifies the type of node that is being registered. The parameter is optional. The default value is CLIENT. You can specify one of the following values:

Client
: Specifies that the client node is a Backup-Archive Client, IBM Spectrum Protect for Space Management client, or application client.

NAS
: Specifies that the node is a network-attached storage (NAS) file server whose data is protected by using NDMP operations. The node name cannot be SERVER.
Note: The name of the NAS node must be the same as the data mover. Therefore, the name cannot be changed after a corresponding data mover is defined.

Server
: Specifies that the client node is a source server that is being registered on the target server.

URL
: Specifies the URL of the IBM Spectrum Protect web client that is configured on the client system. You can use the URL in a web browser and in the Operations Center to remotely manage the client node.

This parameter is optional. The URL must include the DNS name or IP address of the client system, and the port number that is defined on the client system for the IBM Spectrum Protect web client. For example,
`http://client.mycorp.com:1581`

UTILITYUrl
: Specifies the address of the IBM Spectrum Protect client management services that are configured on the client system. This URL is used by the Operations Center to access client log files so that you can remotely diagnose client issues from the Operations Center.

  This parameter is optional. You can specify a URL of up to 200 characters in length. The URL must start with `https`. It includes the DNS name or IP address of the client system, and the port number that is defined on the client system for the IBM Spectrum Protect client management services. For example, `https://client.mycorp.com:9028`

  If you omit the port number, the Operations Center uses the port number 9028, which is the default port number when you install the client management services on the client system.

MAXNUMMP
: Specifies the maximum number of mount points a node is allowed to use on the server or storage agent only for operations such as backup, archive, and IBM Spectrum Protect for Space Management migration. The parameter is optional and does not apply to nodes with a type of NAS or SERVER. The default value is 1. You can specify an integer in the range 0 - 999. A value of 0 specifies that a node cannot acquire any mount point for a client data store operation. The MAXNUMMP value is not evaluated or enforced during client data read operations such as restore, retrieve, and IBM Spectrum Protect for Space Management recall. However, mount points in use for data read operations are evaluated against attempted concurrent data store operations for the same client node and might prevent the data store operations from being able to acquire mount points.

  For volumes in a storage pool that is associated with the FILE or CENTERA device type, the server can have multiple sessions to read and one process to write to the same volume concurrently. To increase concurrency and provide efficient access for nodes with data in FILE or CENTERA storage pools, increase the value of the MAXNUMMP parameter.

  For nodes that store data into primary storage pools with the simultaneous-write function that is enabled, you must adjust the value of the MAXNUMMP parameter to specify the correct number of mount points for each client session. A client session requires one mount point for the primary storage pool and one mount point for each copy storage pool and each active-data pool.

  For server-to-server backup, if one server is at a different version than the other server, set the number of mount points on the target server to a value higher than one. Otherwise, you receive an error.

  A storage agent independently tracks the number of points that are used during a client session. If a node has a storage agent that is installed, it might exceed the MAXNUMMP value. The MAXNUMMP value might also be exceeded under conditions where the node does not have to wait for a mount point.

  Note: The server might preempt a client operation for a higher priority operation and the client might lose a mount point if no other mount points are available.

KEEPMP
: Specifies whether the client node keeps the mount point for the entire session. The parameter is optional. The default value is NO. You can specify one of the following values:

  Yes
  : Specifies that the client node must retain the mount point during the entire session. If policy definitions cause data to be stored to a disk storage pool after the data is stored to a sequential access storage pool, any mount points that are held by the session will not be released.

  No
  : Specifies that the client node releases the mount point during the session. If policy definitions cause data to be stored to a disk storage pool after the data is stored to a sequential access storage pool, any mount points that are held by the session will be released.

AUTOFSRename
: Specify whether file spaces are automatically renamed when you upgrade the client system to support Unicode or specify whether file spaces are renamed by the client, if needed. The parameter is optional. The default is NO. Setting the parameter to YES enables automatic renaming, which occurs when the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup. The automatic renaming changes the names of existing backed-up file spaces that are not in Unicode in server storage. Then, the file spaces are backed up in Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect clients by using Windows, Macintosh OS X, and NetWare operating systems.

  After the client with support for Unicode is installed, any new file spaces that the client backs up are stored in server storage by using the UTF-8 code page. UTF-8 is a byte-oriented encoding form that is specified by the Unicode Standard.

You can specify one of the following values:

Yes
: Existing file spaces are automatically renamed when you upgrade to a client that supports Unicode and the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup. The renaming occurs whether the client uses the graphical user interface, the command line, or the client scheduler.
For example, the server renames a drive as follows:

```
Original name: D_DRIVE
New name: D_DRIVE_OLD
```

The new name indicates that the file space is stored on the server in a format that is not Unicode.

No
: Existing file spaces are not automatically renamed when the client system upgrades to a client that supports Unicode, and the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup.

Client
: The option AUTOFSRENAME in the client's option file determines whether file spaces are renamed.

By default, the client option is set to PROMPT. When the client system upgrades to a client that supports Unicode and the client runs an IBM Spectrum Protect operation with the graphical user interface or the command line, the program displays a one-time prompt to the user about whether to rename file spaces.

When the client scheduler runs an operation, the program does not prompt for a choice about renaming, and does not rename file spaces. Backups of existing file spaces are sent as before (not in Unicode).

VALIdateprotocol (deprecated)
: Specifies whether IBM Spectrum Protect completes a cyclic redundancy check (CRC) to validate the data that is sent between the client and server. The parameter is optional. The default is NO.
Important: Beginning with IBM Spectrum Protect V8.1.2 and Tivoli® Storage Manager Version 7.1.8, this parameter is deprecated. The validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The VALIDATEPROTOCOL parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

TXNGroupmax
: Specifies the number of files per transaction commit that are transferred between a client and a server. The parameter is optional. Client performance might be improved by using a larger value for this option.

The default value is 0. Specifying 0 indicates that the node uses the server global value that is set in the server options file. To use a value other than the server global value, specify a value of 4 through 65,000 for this parameter. The node value takes precedence over the server value.

Attention: Increasing the TXNGROUPMAX value increases the recovery log usage. Higher recovery log usage might increase the risk of running out of log space. Evaluate the performance of each node before you change the parameter.

DATAWritepath
: Specifies the transfer path that is used when the client sends data to the server, storage agent, or both, during storage operations such as backup or archive. The parameter is optional. The default is ANY.
Note: If a path is unavailable, the node cannot send any data. For example, if you select the LAN-free option but a LAN-free path is not defined, the operation fails.

You can specify one of the following values:

ANY
: Specifies that data is sent to the server, storage agent, or both, by any available path. A LAN-free path is used if one is available. If a LAN-free path is unavailable, the data is moved by using the LAN.

LAN
: Specifies that data is sent by using the LAN.

LANFree
: Specifies that data is sent by using a LAN-free path.

DATAReadpath
: Specifies the transfer path that is used when the server, storage agent, or both read data for a client, during operations such as restore or retrieve. The parameter is optional. The default is ANY.

Note: If a path is unavailable, data cannot be read. For example, if you select the LAN-free option but a LAN-free path is not defined, the operation fails. The value for the transfer path also applies to failover connections. If the value is set to LANFree, failover cannot occur for the node on the secondary server.

You can specify one of the following values:

ANY
: Specifies that the server, storage agent, or both use any available path to read data. A LAN-free path is used if one is available. If a LAN-free path is unavailable, the data is read by using the LAN.

LAN
: Specifies that data is read by using the LAN.

LANFree
: Specifies that data is read by using a LAN-free path.

TARGETLevel

Specifies the client deployment package that is targeted for this node. You can substitute an applicable release package for Version.Release.Modification.Fix (V.R.M.F) Level. For example: `TARGETLevel=6.2.0.0`.

You must specify each segment with a number that is applicable to a deployment package. You cannot use an asterisk in any field as a substitution for a valid number. The parameter is optional.
Restriction: The TARGETLEVEL parameter does not apply to nodes with a type of NAS or SERVER.

SESSIONINITiation

Controls whether the server or the client initiates sessions. The default is that the client initiates sessions. The parameter is optional.

Clientorserver
: Specifies that the client might initiate sessions with the server by communicating on the TCP/IP port that is defined with the server option TCPPORT. Server-prompted scheduling might also be used to prompt the client to connect to the server.

SERVEROnly
: Specifies that the server does not accept client requests for sessions. All sessions must be initiated by server-prompted scheduling on the port that is defined for the client with the REGISTER or UPDATE NODE commands. You cannot use the client acceptor, dsmcad, to start the scheduler when SESSIONINITIATION is set to SERVERONLY.

  HLAddress

  Specifies the client IP address that the server contacts to initiate scheduled events. This parameter must be used when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that are previously used by the client to contact the server.

  The address can be specified either in numeric or host name format. If a numeric address is used, it is saved without verification by a domain name server. If the address is not correct, it can cause failures when the server attempts to contact the client. Host name format addresses are verified with a domain name server. Verified names are saved and resolved with Domain Name Services when the server contacts the client.

  LLAddress

  Specifies the client port number on which the client listens for sessions from the server. This parameter must be used when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that are previously used by the client to contact the server.

  The value for this parameter must match the value of client option TCPCLIENTPORT. The default value is 1501.

EMAILADdress
: This parameter is used for more contact information. The parameter is optional. The information that is specified by this parameter is not acted upon by IBM Spectrum Protect.

DEDUPlication
: Specifies where data deduplication can occur for this node. The parameter is optional. You can specify one of the following values:

  Clientorserver
  : Specifies that data that is stored by this node can be deduplicated on either the client or the server. This value is the default. For data deduplication to take place on the client, you must also specify a value of YES for the

DEDUPLICATION client option. You can specify this option in the client option file or in the client option set on the IBM Spectrum Protect server.

SERVEROnly
: Specifies that data that is stored by this node can be deduplicated on the server only.

BACKUPINITiation
: Specifies whether the non-root user ID on the client node can back up files to the server. The parameter is optional. The default value is ALL, indicating that non-root user IDs can back up data to the server. You can select one of the following values:

  All
  : Specifies that non-root user IDs can back up files to the server. ALL is the default if BACKUPINITIATION is not specified.

  ROOT
  : Specifies that the root user ID can back up files to the server. If you are using the V6.4 or later backup-archive client, authorized users have the same privileges as the root user ID.
    Restriction: The attribute is ignored by the server if the backup-archive client connects from an operating system other than AIX, Linux, or Mac OS.
    Remember: The application programming interface (API) is affected by the BACKUPINITIATION parameter on the server. By default, all API users are allowed to back up data. Setting the parameter to `ROOT` on an API node is not recommended.

REPLState
: Specifies whether data that belongs to the client node is ready to be replicated. This parameter is optional. Specify this parameter only if you are issuing the REGISTER NODE command on a server that is configured to replicate data to a target replication server. If you register a client node on a source replication server and set up replication for the node, do not register the node on the target replication server. The client node is created automatically on the target server the first time that replication occurs.
  You can select one of the following values:

  ENabled
  : Specifies that the client node is configured for replication and is ready to replicate. When you specify this parameter, the replication mode in the client node definition on the source replication server is automatically set to SEND. This setting indicates that data that belongs to the client node is sent to a target server during replication.

    When replication first occurs for the client node, the replication state of the node on the target replication server is automatically set to ENABLED. The replication mode on the target replication server is set to RECEIVE. This setting indicates that data that belongs to the client node is received from a source replication server. To determine the replication state and mode, issue the QUERY NODE command on a source or a target replication server.

  DISabled
  : Specifies that the node is configured for replication but that replication does not occur until you enable it.

BKREPLRuledefault, ARREPLRuledefault, and SPREPLRuledefault
: Specifies the replication rule that applies to a data type if the file space rules for the data type are set to DEFAULT.
  Restriction: You can specify the BKREPLRULEDEFAULT, ARREPLRULEDEFAULT, or SPREPLRULEDEFAULT parameter only if you specify the REPLSTATE parameter.

  BKREPLRuledefault
  : Specifies the replication rule for backup data.

  ARREPLRuledefault
  : Specifies the replication rule for archive data.

  SPREPLRuledefault
  : Specifies the replication rule for space-managed data.

  If the file space rules for the data type are set to DEFAULT and you do not specify a rule for the BKREPLRULEDEFAULT, ARREPLRULEDEFAULT, or SPREPLRULEDEFAULT parameter, data is replicated according to the server rule for the data type.

  You can specify normal-priority replication or high-priority replication rules. In a replication process that includes both normal and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

  You can specify the following rules:

  ALL_DATA

Replicates active and inactive backup data, archive data, or space-managed data. The data is replicated with a normal priority.

ACTIVE_DATA
: Replicates only active backup data. The data is replicated with a normal priority. This rule is valid only for BKREPLRULEDEFAULT.
Attention:

  If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

  - When a release version earlier than Version 7.1.1 is installed on either the source or target replication servers.
  - When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
  - When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a release version earlier than V7.1.1.

  If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
: Replicates active and inactive backup data, archive data, or space-managed data. Data is replicated with a high priority.

ACTIVE_DATA_HIGH_PRIORITY
: This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority. This rule is valid only for BKREPLRULEDEFAULT.

DEFAULT
: Replicates data according to the server replication rule for backup data.

  For example, suppose that you want to replicate the archive data in all the file spaces that belongs to a client node. Replication of the archive data is a high priority. One method to accomplish this task is to specify `ARREPLRULEDEFAULT=DEFAULT`. Ensure that the file space rules for archive data are also set to DEFAULT and that the server rule for archive data is set to ALL_DATA_HIGH_PRIORITY.

  Restriction: If a node is configured for replication, the file space rules are set to DEFAULT after the node stores data on the source replication server.

NONE
: Data of the specified type is not replicated.

  For example, if you do not want to replicate space-managed data that belongs to a client node, specify `SPREPLRULEDEFAULT=NONE`

RECOVERDamaged
: Specifies whether damaged files can be recovered for this node from a target replication server. The parameter is optional. The default value is YES. You can specify one of the following values:

  Yes
  : Specifies that recovery of damaged files from a target replication server is enabled for this node.

  No
  : Specifies that recovery of damaged files from a target replication server is not enabled for this node.
  Tip: The value of the RECOVERDAMAGED parameter is only one of several settings that determine whether damaged files are recovered. For information about how to specify the settings, see Settings that affect the recovery of damaged files.

ROLEOVERRIDE

: Specifies whether to override the reported role of the client for processor value unit (PVU) estimation reporting. The default is USEREPORTED. The parameter is optional.

  The role reported by the client is either client-device (for example, a workstation) or server-device (for example, file/print server, application server, database). By default, the client reports its role that is based on the client type and the operating system. All clients initially report their role as server-device, except for Backup-Archive Clients running Microsoft Windows workstation distributions (Windows Vista) and Macintosh OS X.

  Specify one of the following values:

  Client
  : Specifies a client-device.

Server
Specifies a server-device.
Other
Specifies that this node is not to be used for PVU estimation reporting. This value can be useful when multiple nodes are deployed for a physical system (for example, virtual environments, test nodes, retired nodes, and nodes not in production or clustering).
Usereported
Use the reported role that is provided by the client.

AUTHentication
This parameter specifies the password authentication method for the node. Specify one of the following values: LDAP or LOCAL. The parameter is optional and defaults to LOCAL. The default can change to LDAP if you use the SET DEFAULTAUTHENTICATION command and specify LDAP.

LOcal
Specifies that the local IBM Spectrum Protect server database is used.
LDap
Specifies that the node uses an LDAP server for password authentication.

SSLrequired (deprecated)

Specifies whether the node must use the Secure Sockets Layer (SSL) protocol to communicate with the IBM Spectrum Protect server. The parameter is optional. When you authenticate passwords with an LDAP directory server, you must protect the sessions by using SSL or another network security method.

Important: Beginning with IBM Spectrum Protect V8.1.2 software and Tivoli Storage Manager V7.1.8 software, this parameter is deprecated. The validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The SSLREQUIRED parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

SESSIONSECurity
Specifies whether the node must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

You can specify one of the following values:

STRict
Specifies that the strictest security settings are enforced for the node. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the server and the node. To specify whether the server uses TLS 1.2 for the entire session or only for authentication, see the SSL client option.
To use the STRICT value, the following requirements must be met to ensure that the node can authenticate with the server:

- Both the node and server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
- The node must be configured to use the TLS 1.2 protocol for SSL sessions between the server and the node.

Nodes set to STRICT that do not meet these requirements are unable to authenticate with the server.
TRANSitional
Specifies that the existing security settings are enforced for the node. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the node has never met the requirements for the STRICT value, the node will continue to authenticate by using the TRANSITIONAL value. However, after a node meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the node can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after a node successfully authenticates by using a more secure communication protocol, the node can no longer authenticate by using a less secure protocol. For example, if a node that is not using SSL is updated and successfully authenticates by using TLS 1.2, the node can no longer authenticate by using no SSL protocol or by using TLS 1.1. This restriction also applies when you use functions such as virtual volumes, when the node authenticates to the IBM Spectrum Protect server as a node from another server.

SPLITLARGEObjects
Specifies whether large objects that are stored by this node are automatically split into smaller pieces, by the server, to optimize server processing. The parameter is optional. Specifying Yes causes the server to split large objects (over 10 GB)

into smaller pieces when stored by a client node. Specifying No bypasses this process. Specify No only if your primary concern is maximizing throughput of backups directly to tape. The default value is Yes.

Example: Register a client node that only the root user can back up

Register the client node `mete0rite` with password *KingK0ng* to back up files from only the root user to the server.

```
register node mete0rite KingK0ng
backupinit=root
```

Example: Register a client node and password and set compression on

Register the client node `JOEOS2` with the password *SECRETCODE* and assign this node to the `DOM1` policy domain. This node can delete its own backup and archive files from the server. All files are compressed by the client node before they are sent to the server. This command automatically creates a `JOEOS2` administrative user ID with password *SECRETCODE*. In addition, the administrator now has client owner authority to the `JOEOS2` node.

```
register node joeos2 secretcode domain=dom1
 archdelete=yes backdelete=yes
 compression=yes
```

Example: Grant client owner authority for an existing administrative user

Grant client owner authority to an existing administrative user ID, `HELPADMIN`, when you register the client node `JAN`. This step would not automatically create an administrator ID named `JAN`, but would grant client owner authority for this node to the `HELPADMIN` administrator.

```
register node jan pwd1safe userid=helpadmin
```

Example: Register a NAS file server node that uses NDMP operations

Register a node name of `NAS1` for a NAS file server that is using NDMP operations. Assign this node to a special NAS domain.

```
register node nas1 pwd4nas1 domain=nasdom type=nas
```

Example: Register a node and specify the maximum number of files per transaction commit

Register a node name of `ED` and set the TXNGroupmax to 1000.

```
register node ed pw459twx txngroupmax=1000
```

Example: Register a node and allow it to deduplicate data on the client system

Register a node name of `JIM` and allow it to deduplicate data on the client system.

```
register node jim jimspass deduplication=clientorserver
```

Example: Register a node name of ED and set the role as a server-device for PVU estimation reporting

Register a node name of `ED` and set the role as a server-device for PVU estimation reporting.

```
register node ed pw459twx roleoverride=server
```

Example: Register a node on a source replication server

Define NODE1 to a source replication server. Specify a replication rule for the backup data that belongs to NODE1 so that active backup data is replicated with a high priority. Enable replication for the node.

```
register node node1 bkreplruledefault=active_data_high_priority replstate=enabled
```

Example: Register a node that authenticates with an LDAP server

Register a node name of NODE17 that must authenticate with an LDAP server.

```
register node node1pwd authentication=ldap
```

Tip: When you register a node in this way, an administrative user ID is not created.

Example: Register a node to communicate with a server by using strict session security

Register a node name of NODE4 to use the strictest security settings to authenticate with the server.

```
register node node4pwd sessionsecurity=strict
```

Example: Register a node and enable recovery of damaged files

Register a node name of PAYROLL. For the PAYROLL node, enable the recovery of damaged files from a target replication server.

```
register node payroll recoverdamaged=yes
```

Related commands

Table 2. Commands related to REGISTER NODE

Command	Description
DEFINE ASSOCIATION	Associates clients with a schedule.
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE MACHNODEASSOCIATION	Associates an IBM Spectrum Protect node with a machine.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
LOCK NODE	Prevents a client from accessing the server.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY PVUESTIMATE	Displays an estimate of the client-devices and server-devices being managed.
QUERY REPLNODE	Displays information about the replication status of a client node.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
REMOVE REPLNODE	Removes a node from replication.
RENAME NODE	Changes the name for a client node.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
RESET PASSEXP	Resets the password expiration for nodes or administrators.
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
SET CPUINFOREFRESH	Specifies the number of days between client scans for workstation information used for PVU estimates.
SET DEDUPVERIFICATIONLEVEL	Specifies the percentage of extents verified by the server during client-side deduplication.

Command	Description
SET REPLRECOVERDAMAGED	Specifies whether node replication is enabled to recover damaged files from a target replication server.
UNLOCK NODE	Enables a locked user in a specific policy domain to access the server.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE NODE	Changes the attributes that are associated with a client node.

Related concepts:

UNIX and Linux client root and authorized user tasks

Related reference:

Ssl client option

REMOVE commands

Use the REMOVE commands to remove an object from IBM Spectrum Protect™.

- REMOVE ADMIN (Delete an administrative user ID)
- AIX Linux Windows REMOVE DAMAGED (Remove damaged data from a source storage pool)
- REMOVE NODE (Delete a node or an associated machine node)
- REMOVE REPLNODE (Remove a client node from replication)
- REMOVE REPLSERVER (Remove a replication server)

REMOVE ADMIN (Delete an administrative user ID)

Use this command to remove an administrative user ID from the system.

You cannot remove the last system administrative user ID or the SERVER_CONSOLE administrative ID from the system.

For users of Lightweight Directory Access Protocol (LDAP) servers: The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                              .-SYNCldapdelete--=--No------.
>>-REMove Admin--admin_name--+----------------------------+----><
                              '-SYNCldapdelete--=--+-No--+-'
                                                   '-Yes-'
```

Parameters

admin_name (Required)
: Specifies the administrative user ID to be removed.

SYNCldapdelete
: Specifies whether to delete the administrative user ID on the Lightweight Directory Access Protocol (LDAP) server.

  Yes
  : Deletes the administrative user ID on the LDAP server.
    Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

  No

Does not delete the administrative user ID on the LDAP server. This is the default value.

Example: Remove an administrative user ID

Remove an administrative user ID larry that is not defined on an LDAP server. Issue the following command:

```
remove admin larry
```

Related commands

Table 1. Commands related to REMOVE ADMIN

Command	Description
LOCK ADMIN	Prevents an administrator from accessing IBM Spectrum Protect.
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
RENAME ADMIN	Changes an IBM Spectrum Protect administrator's name.

AIX | Linux | Windows

REMOVE DAMAGED (Remove damaged data from a source storage pool)

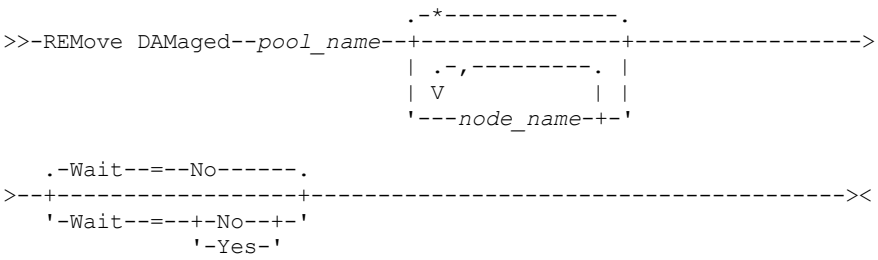
After storage pool conversion, use this command to remove damaged data from a storage pool that uses a FILE device class, a tape device class, or a virtual tape library (VTL).

The REMOVE DAMAGED command permanently deletes damaged data from the storage pool.
Tip: Before you remove damaged data from the storage pool, try to recover an undamaged version of the data from a copy or active-data storage pool by issuing the RESTORE STGPOOL command. Recover an undamaged version of the data from a target replication server by issuing the REPLICATE NODE command and specifying the RECOVERDAMAGED=YES parameter.

Privilege class

To issue this command, you must have restricted storage privilege.

Syntax



Parameters

pool_name (Required)
: Specify a primary storage pool that uses a FILE device class, a tape device class, or a virtual tape library (VTL). The storage pool contains the damaged data. This parameter is required.

node_name
: Specifies the name of the client node. Separate multiple names with commas and no intervening spaces. You can use a wildcard character instead of a node name if you want to remove damage from all of the nodes in the storage pool.

Wait
: Specifies whether to wait for the server to remove damaged data from the storage pool. This parameter is optional. The default value is NO. You can specify this parameter only from an administrative command line. You can specify one of the

following values:

No
: Specifies that the command processes run in the background.

Yes
: Specifies that the command processes run in the foreground. Messages are not displayed until the command completes processing.

Example: Remove damaged data from a storage pool and wait for the server to complete processing

Remove damaged data from a storage pool that is named POOL1 and wait for the server to complete processing in the foreground.

```
remove damaged pool1 wait=yes
```

Table 1. Commands related to REMOVE DAMAGED

Command	Description
CONVERT STGPOOL	Convert a storage pool to a directory-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
REPAIR STGPOOL	Repairs a directory-container storage pool.

REMOVE NODE (Delete a node or an associated machine node)

Use this command to remove a node from the server. If you are using disaster recovery manager and the node to be removed is associated with a machine, the association between the node and the machine is also deleted.

If a node is part of a collocation group and you remove the node from the server, the node is removed from the collocation group. If a node is removed and the node contained file spaces in a file space collocation group, those file spaces are removed from the group member list.

If you remove a node that stored data in a deduplicated storage pool, the node name DELETED is displayed in the QUERY OCCUPANCY command output until all data deduplication dependencies are removed.

When a node is removed, the corresponding administrative ID is removed only if the following issues are true:

- The administrator name is identical to the node name.
- The administrator has client owner or client access authority *only* to the node that is being removed.
- The administrator is not a managed object.

Before you can remove a node, you must delete all backup and archive file spaces that belong to that node.
Before you can remove a NAS node that has a corresponding data mover, you must complete the following tasks in order:

1. Delete any paths from the data mover
2. Delete the data mover
3. Delete all virtual file space definitions for the node
4. Remove the NAS node

For users of Lightweight Directory Access Protocol (LDAP) servers: The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax

```
                          .-SYNCldapdelete--=--No------.
>>-REMove Node--node_name--+----------------------------+------><
                          '-SYNCldapdelete--=--+-No--+-'
```

```
'-Yes-'
```

Parameters

node_name (Required)
: Specifies the name of the node to be removed.

SYNCldapdelete
: Specifies whether to remove the node from the Lightweight Directory Access Protocol (LDAP) server.

  Yes
  : Specifies that the node is removed.
    Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

  No
  : Specifies that the node is not removed. This is the default value.

Example: Remove a client node

Remove the client node LARRY.

```
remove node larry
```

Related commands

Table 1. Commands related to REMOVE NODE

Command	Description
AIX Windows DELETE MACHNODEASSOCIATION	AIX Windows Deletes association between a machine and node.
DELETE DATAMOVER	Deletes a data mover.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
DELETE PATH	Deletes a path from a source to a destination.
DELETE VIRTUALFSMAPPING	Delete a virtual file space mapping.
LOCK NODE	Prevents a client from accessing the server.
QUERY COLLOCGROUP	Displays information about collocation groups.
AIX Windows QUERY MACHINE	AIX Windows Displays information about machines.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY SESSION	Displays information about all active administrator and client sessions with IBM Spectrum Protect.
REGISTER NODE	Defines a client node to the server and sets options for that user.
RENAME NODE	Changes the name for a client node.

REMOVE REPLNODE (Remove a client node from replication)

Use this command to remove a node from replication if you no longer want to replicate the data that belongs to the node.

You cannot delete client node data by issuing the REMOVE REPLNODE command. You can issue the command on a source or on a target replication server. You can only issue this command from an administrative command-line client. You cannot issue this command from the server console.

If you issue the REMOVE REPLNODE command for a client node whose replication mode is set to SEND or RECEIVE, the mode is set to NONE. The replication state is also set to NONE. After you remove a client node from replication, the target replication

server can accept backup, archive, and space-managed data directly from the node.

If a client node is removed from replication, information in the database about replication for the node is deleted. If the client node is enabled for replication later, the replication process replicates all the data that is specified by replication rules and settings.

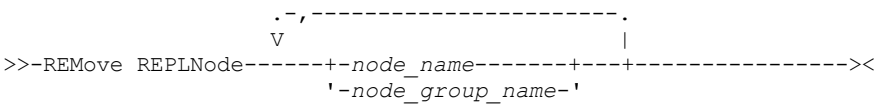
When you issue the REMOVE REPLNODE command, the data that belongs to a client node is not deleted. To delete file space data that belongs to the client node, issue the DELETE FILESPACE command for each of the file spaces that belong to the node. If you do not want to keep the client node definition, issue the REMOVE NODE command. To delete file space data and the client node definition, issue DELETE FILESPACE and REMOVE NODE on the target replication server.

Restriction: If a node replication process is running for a client node that is specified by this command, the command fails and the replication information for the node is not removed.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax



Parameters

node_name or node_group_name (Required)
: Specifies the name of the client node or defined group of client nodes that you want to remove from replication. To specify multiple client node names and client-node group names, separate the names with commas and no intervening spaces. You can use wildcard characters to specify client node names, but not to specify client-node group names. You cannot combine node or node group names with the domain name.

Example: Remove three client nodes and a client node group from replication

The names of the client nodes are NODE1, NODE2, and NODE3. The name of the client node group is PAYROLL. Issue the following command on the source and target replication servers:

```
remove replnode node*,payroll
```

Related commands

Table 1. Commands related to REMOVE REPLNODE

Command	Description
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.

REMOVE REPLSERVER (Remove a replication server)

Use this command to remove or to switch to a replication server from the list of replication servers. This command deletes all information about replication state for all nodes that were replicated to that server.

You can issue the command on a source or on a target replication server.
Restriction: You cannot delete client node data by using the REMOVE REPLSERVER command.

Use the command to switch replication servers and to remove replication information for an old server. The command does not affect the current replication mode or state of any node definitions. Issue the command on both the source and target servers to keep the replication state information about both servers consistent.

Restriction: If you specify the default replication server for the REMOVE REPLSERVER command and a node replication process is running, the command fails and no replication information is removed.

This command runs as a background operation and it cannot be canceled. IBM Spectrum Protect™ deletes replication information that is associated with the specified server as a series of batch database transactions. If a system failure occurs, a partial deletion can occur.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-REMove REPLServer--GUID-------------------------------------><
```

Parameters

replication_guid (Required)

The unique identifier for the replication server that is being removed. You can use wildcards to specify the Replication Global Unique Identifier (GUID), however, only one GUID can match the wildcard. If the wildcard sequence matches more than one GUID, the command fails. You must qualify the wildcard string until only the GUID that you want to delete is found.

Example: Use a wildcard to remove a replication server

Remove a replication server by using a wildcard character to indicate the GUID.

```
remove replserver e*
```

Related commands

Table 1. Commands related to REMOVE REPLSERVER

Command	Description
REMOVE REPLNODE (Remove a client node from replication)	Removes a node from replication.
QUERY REPLSERVER (Query a replication server)	Displays information about replicating servers.

RENAME commands

Use the RENAME commands to change the name of an existing object.

- RENAME ADMIN (Rename an administrator)
- RENAME FILESPACE (Rename a client file space on the server)
- RENAME NODE (Rename a node)
- RENAME SCRIPT (Rename an IBM Spectrum Protect script)
- RENAME SERVERGROUP (Rename a server group)
- RENAME STGPOOL (Change the name of a storage pool)

RENAME ADMIN (Rename an administrator)

Use this command to change an administrative user ID. Existing information for this administrator such as password, contact information, and privilege classes is not altered.

If you assign an existing administrative user ID to another person, use the UPDATE ADMIN command to change the password.

When an administrator and a node share a name and you change the administrator authentication method, the node authentication method also changes. If you rename an administrator to the same name as an existing node, the authentication

method and the SSLREQUIRED setting for the node can change. If those settings are different, after the renaming, both administrator and node will have the same authentication method and SSLREQUIRED setting.

For users of Lightweight Directory Access Protocol (LDAP) servers:

- The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
- Do not rename an administrative user ID to match a node name. If the names match, you might see unexpected behavior because of automatic password changes that update the same password twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update might fail.

You cannot rename the SERVER_CONSOLE administrative ID.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-REName Admin--current_admin_name--new_admin_name------------>

   .-SYNCldapdelete--=--No------.
>--+----------------------------+------------------------------><
   '-SYNCldapdelete--=--+-No--+-'
                        '-Yes-'
```

Parameters

current_admin_name (Required)
: Specifies the administrative user ID to be renamed.

new_admin_name (Required)
: Specifies the new administrative user ID. The maximum length of the name is 64 characters.

SYNCldapdelete
: Specifies whether to delete the administrative user ID on the Lightweight Directory Access Protocol (LDAP) server and replace the ID with a new one.

  Yes
  : Deletes the administrative user ID on the LDAP server and replaces it with a new ID.
    Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

  No
  : Does not delete and replace the administrative user ID on the LDAP server. This is the default value.

Example: Rename an administrator

Rename the IBM Spectrum Protect administrator CLAUDIA to BILL.

```
rename admin claudia bill
```

Related commands

Table 1. Commands related to RENAME ADMIN

Command	Description
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.

RENAME FILESPACE (Rename a client file space on the server)

Use this command to rename an existing client file space on the server to a new file space name or to rename imported file spaces.

You might want to rename a file space that was imported or to cause the creation of new Unicode-enabled file spaces for Unicode-enabled clients.

Restriction: Do not rename NAS or VMware file spaces. If you rename a NAS or VMware file space, it is no longer visible and cannot be restored. To restore a renamed NAS or VMware file space, you must rename it back to its original name and set the force parameter as follows:force=yes

Privilege class

Any administrator with unrestricted policy authority or with restricted policy authority over the client's policy domain can issue this command.

Syntax

```
>>-REName FIlespace--node_name----------------------------------->

>--current_file_space_name--new_file_space_name----------------->

   .-NAMEType--=--SERVER------.
>--+--------------------------+-------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-NEWNAMEType--=--SERVER----------.
>--+-------------------------------+--+---------------+------><
   |                           (1)   |  '-force--=--yes-'
   '-NEWNAMEType--=--+-UNIcode-----+-'
                     '-HEXadecimal-'
```

Notes:

1. This parameter is the default when you specify NAMEType=UNIcode.

Parameters

node_name (Required)
: Specifies the name of the client node to which the file space to be renamed belongs.

current_file_space_name (Required)
: Specifies the name of the file space to be renamed. A file space name is case-sensitive and must be specified exactly as defined to the server. Virtual file space mapping names are allowed.

new_file_space_name (Required)
: Specifies the new name for the file space. A client file space name is case-sensitive and must be specified exactly as it is to be defined to the server. This parameter cannot be an existing virtual file space mapping name. If the current_file_space_name is a virtual file space, the new_file_space_name must follow all the rules for defining a virtual file space name. See the DEFINE VIRTUALFSMAPPING command for more information.
Important: If the new name type is hexadecimal, specify valid UTF-8 hexadecimal values so the server's code page displays the file space name as intended. For example, do not specify a value that can be interpreted as a backspace.
When you rename a file space that is part of a file space collocation group, the collocation group is updated with the new name.

NAMEType
: Specify how you want the server to interpret the current file space name that you enter. This parameter is useful when the server has clients with support for Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect™ clients with Windows, Macintosh OS X, and NetWare operating systems.

  The default value is SERVER. If a virtual file space mapping name is specified, you must use SERVER. Possible values are:

  SERVER
  : The server uses the server's code page to interpret the file space name.

  UNIcode

The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.

FSID
The server interprets the file space name as the file space ID (FSID).

NEWNAMEType
Specify how you want the server to interpret the new file space name that you enter. The default is SERVER if you specified the NAMETYPE as SERVER, or if the file space to be renamed is not Unicode. The default is UNICODE if you specified the NAMETYPE as UNICODE, or if the file space to be renamed is Unicode. If a virtual file space mapping name is specified, you must use SERVER. Possible values are:

SERVER
The server uses the server's code page to interpret the file space name.

UNIcode
The server converts the file space name that is entered from the server code page, to the UTF-8 code page. The success of the conversion depends on the actual characters in the name and the server's code page. If the conversion is not successful, you might want to specify the HEXADECIMAL parameter.

HEXadecimal
The server interprets the file space name that you enter as the hexadecimal representation of a name in Unicode. Using hexadecimal ensures that the server is able to correctly rename the file space, regardless of the server's code page.
To view the hexadecimal representation of a file space name, you can use the QUERY FILESPACE command with FORMAT=DETAILED.
Restriction: You cannot specify a new name of a type that is different from the original name. You can rename a file space that is Unicode to another name in Unicode. You can rename a file space that is not Unicode, and use a new name in the server's code page. You cannot mix the two types.

force
To rename a NAS or VMware file space you must set this parameter as follows: force=yes

Rename an imported file space to prevent overwriting

An AIX® client node named LARRY backed up file space /r033 to the IBM Spectrum Protect server. The file space was exported to tape and later reimported to the server. When this file space was imported, a system-generated name, /r031, was created for it because /r033 existed for client node LARRY.

Client node LARRY, however, already had a file space named /r031 that was not backed up, therefore, was unknown to the server. Unless the imported file space is renamed, it overlays file space /r031 because the file space name generated by the IMPORT function is the same as a file space on client node LARRY that is unknown to the server.

Use the following command to rename imported file space /r031. The new name, /imported-r033, identifies that the new file space is an imported image of file space /r033.

```
rename filespace larry /r031 /imported-r033
```

Rename file space to create a Unicode-enabled file space

Client JOE is using an English Unicode-enabled IBM Spectrum Protect client. JOE backed up several large file spaces that are not Unicode that is enabled in server storage. File space \\joe\c$ contains some files with Japanese file names that cannot be backed up to a file space that is not Unicode that is enabled. Because the file spaces are large, the administrator does not want to convert all of JOE's file spaces to Unicode-enabled file spaces now. The administrator wants to rename only the non-Unicode file space, \\joe\c$, so that the next backup of the file space causes the creation of a new Unicode-enabled file space. The new Unicode-enabled file space allows the Japanese files to be successfully backed up.

Use the following command to rename \\joe\c$:

```
rename filespace joe \\joe\c$ \\joe\c$_old
```

Related commands

Table 1. Commands related to RENAME FILESPACE

Command	Description
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
EXPORT NODE	Copies client node information to external media or directly to another server.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY OCCUPANCY	Displays file space information by storage pool.

RENAME NODE (Rename a node)

Use this command to rename a node.

If you are assigning an existing node ID to another person, use the UPDATE NODE command to change the password.

For users of Lightweight Directory Access Protocol (LDAP) servers:

- The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
- Do not rename a node to match an existing administrative user ID. If you rename a node, and the node name matches an administrative user ID, you might see unexpected behavior because of automatic password changes that update the same password twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update might fail.

Restrictions:

- You cannot rename a NAS node name that has a corresponding data mover defined. If the data mover has defined paths, the paths must first be deleted.
- If a node is configured for replication, it cannot be renamed.

If you rename a node to the same name as an existing administrator, the administrator authentication method and SSLREQUIRED setting are updated to match the node. When a node and an administrator share a name and you change the node authentication method or the node SSLREQUIRED setting, the administrator settings also change. You must have system level authority to update the node authentication method or the node SSLREQUIRED setting and also update a same-named administrator.

Privilege class

You must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax

```
>>-REName Node--current_node_name--new_node_name---------------->

   .-SYNCldapdelete--=--No------.
>--+----------------------------+------------------------------><
   '-SYNCldapdelete--=--+-No--+-'
                        '-Yes-'
```

Parameters

current_node_name (Required)
: Specifies the name of the node to be renamed.

new_node_name (Required)
: Specifies the new name of the node. The maximum length is 64 characters.

SYNCldapdelete
Specifies whether the node name is deleted and replaced on the Lightweight Directory Access Protocol (LDAP) server.

Yes
Specifies that the node name is deleted and replaced.
Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

No
Specifies that the node name is not deleted and replaced. This is the default value.

Example: Rename a node

Rename the node JOE to JOYCE.

```
rename node joe joyce
```

Example: Rename a node that shares a namespace with other servers

Rename the node JOYCE to JOE and do not delete the previous name from corresponding LDAP servers.

```
rename node joyce joe
```

Related commands

Table 1. Commands related to RENAME NODE

Command	Description
QUERY NODE	Displays partial or complete information about one or more clients.
UPDATE NODE	Changes the attributes that are associated with a client node.

Related tasks:
Managing NAS file server nodes

RENAME SCRIPT (Rename an IBM Spectrum Protect script)

Use this command to rename an IBM Spectrum Protect™ script.

Privilege class

To issue this command, you must have operator, policy, system, storage, or system privilege.

Syntax

```
>>-REName SCRipt--current_script_name--new_script_name --------><
```

Parameters

current_script_name (Required)
Specifies the name of the script to rename.

new_script_name (Required)
Specifies the new name for the script. The name can contain as many as 30 characters.

Example: Rename a script

Rename SCRIPT1 to a new script named SCRIPT2.

```
rename script script1 script2
```

Related commands

Table 1. Commands related to RENAME SCRIPT

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
QUERY SCRIPT	Displays information about scripts.
RUN	Runs a script.
UPDATE SCRIPT	Changes or adds lines to a script.

RENAME SERVERGROUP (Rename a server group)

Use this command to rename a server group.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-REName SERVERGroup--current_group_name--new_group_name------><
```

Parameters

current_group_name (Required)
: Specifies the server group to rename.

new_group_name (Required)
: Specifies the new name of the server group. The maximum length of the name is 64 characters.

Example: Rename a server group

Rename server group WEST_COMPLEX to BIG_WEST.

```
rename servergroup west_complex big_west
```

Related commands

Table 1. Commands related to RENAME SERVERGROUP

Command	Description
COPY SERVERGROUP	Creates a copy of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE SERVERGROUP	Deletes a server group.
QUERY SERVERGROUP	Displays information about server groups.
UPDATE SERVERGROUP	Updates a server group.

RENAME STGPOOL (Change the name of a storage pool)

Use this command to change the name of a storage pool. You can change storage pool names to use the same names on a configuration manager and its managed servers.

When you rename a storage pool, any administrators with restricted storage privilege for the old storage pool automatically retain restricted storage privilege for the renamed storage pool. If the renamed storage pool is in a storage pool hierarchy, the hierarchy

is preserved. You must update the management class or copy group to specify the new storage pool name as the destination for files.

If processes are active when a storage pool is renamed, the old name might still be displayed in messages or queries for those processes.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-RENname STGpool--current_pool_name--new_pool_name------------><
```

Parameters

current_pool_name (Required)
: Specifies the storage pool to rename.

new_pool_name (Required)
: Specifies the new name of the storage pool. The maximum length of the name is 30 characters.

Example: Change the name of a storage pool

Rename storage pool STGPOOLA to STGPOOLB:

```
rename stgpool stgpoola stgpoolb
```

Related commands

Table 1. Commands related to RENAME STGPOOL

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE STGPOOL	Deletes a storage pool from server storage.
QUERY STGPOOL	Displays information about storage pools.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
UPDATE STGPOOL	Changes the attributes of a storage pool.

AIX Linux Windows

REPAIR STGPOOL (Repair a directory-container storage pool)

Use this command to repair deduplicated extents in a directory-container storage pool. Damaged deduplicated extents are repaired with extents that are backed up to the target replication server or to container-copy storage pools on the same server.

Restrictions:

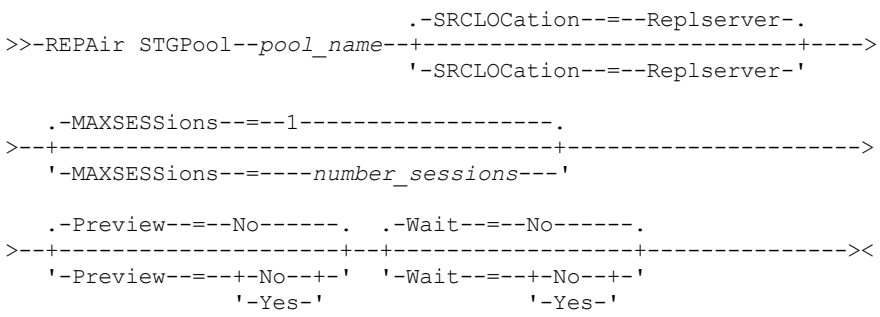
- You can issue the REPAIR STGPOOL command only if you already issued the PROTECT STGPOOL command to back up data to another storage pool on a replication target server or on the same server.
- When you repair a directory-container storage pool from the replication server, the REPAIR STGPOOL command fails when any of the following conditions occur:
  - The target server is unavailable.
  - The target storage pool is damaged.
  - A network outage occurs.
- When you repair a directory-container storage pool from container-copy pools, the REPAIR STGPOOL command fails when any of the following conditions occur:

- The container-copy storage pool is unavailable.
- The container-copy storage pool is damaged.

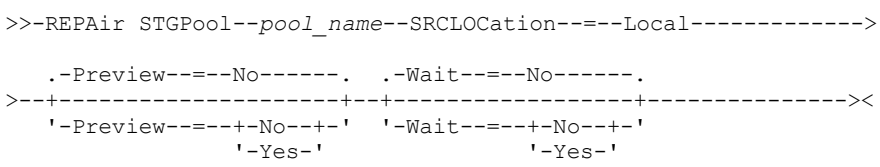
Privilege class

To issue this command, you must have system privilege.

Syntax when the source is the replication server



Syntax when the source is a storage pool on the same server



Parameters

pool_name (Required)
: Specifies the name of the directory-container storage pool that contains the data that must be repaired.

SRCLOCation
: Specifies the source location that is used to repair the data. The default value is REPLSERVER. This parameter is only required when the source location is on the same server. You can specify one of the following values:

  Local
  : Specifies that the data is repaired from container-copy storage pools on the same server.

  Replserver
  : Specifies that the data is repaired from a directory-container storage pool on the target replication server.

MAXSESSions
: Specifies the maximum number of data sessions that can send data to a target server. This parameter is optional when you repair data from a replication server.
  The value that you specify can be in the range 1 - 20. The default value is 1. If you increase the number of sessions, you can repair the storage pool faster.

  When you set a value for the MAXSESSIONS parameter, ensure that the available bandwidth and the processor capacity of the source and target servers are sufficient.

  Tips:

  - If you issue a QUERY SESSION command, the total number of sessions might exceed the number of data sessions.
  - The number of sessions that are used to repair storage pools depends on the amount of data that is repaired. If you repair only a small amount of data, there is no benefit to increasing the number of sessions.

Preview
: Specifies whether to preview data or to repair the data. This parameter is optional. The default value is NO. You can specify one of the following values:

No
Specifies that the data is repaired to the storage pool but the data is not previewed.

Yes
Specifies that the data is previewed but not repaired.

Wait
Specifies whether to wait for the server to complete the repair processing of the storage pool. This parameter is optional. The default value is NO. You can specify this parameter only from an administrative command line. You can specify one of the following values:

No
Specifies that the command processes run in the background. To monitor the background processing of the REPAIR STGPOOL command, issue the QUERY PROCESS command.

Yes
Specifies that the command processes run in the foreground. Messages are not displayed until the command completes processing.

Example: Repair a storage pool and preview the data

Repair a storage pool that is named POOL1 and preview the data.

```
repair stgpool pool1 preview=yes
```

Example: Repair a storage pool and specify a maximum number of sessions

Repair a storage pool that is named POOL1 and specify 10 maximum sessions.

```
repair stgpool pool1 maxsessions=10
```

Example: Repair a storage pool from tape

Repair a storage pool that is named POOL1 and specify local for the source location.

```
repair stgpool pool1 SRCLOCation=local
```

Table 1. Commands related to REPAIR STGPOOL

Command	Description
DEFINE STGPOOL (directory-container)	Define a directory-container storage pool.
DEFINE STGPOOL (container-copy)	Define a container-copy storage pool that stores copies of data from a directory-container storage pool.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.

REPLICATE NODE (Replicate data in file spaces that belong to a client node)

Use this command to replicate data in file spaces that belong to one or more client nodes or defined groups of client nodes.

When you issue this command, a process is started in which data that belongs to the specified client nodes is replicated according to replication rules. Files that are no longer stored on the source replication server, but that exist on the target replication server, are deleted during this process.
Tip: Avoid conflicts in managing administrative IDs and client option sets by identifying the IDs and option sets that are replicated to the target server and the IDs and option sets that are managed in an enterprise configuration. You cannot define an administrative user ID for a registered node if an administrative ID exists for the same node.

If a node replication process is already running for a client node that is specified by this command, the node is skipped, and replication begins for other nodes that are enabled for replication.

After the node replication process is completed, a recovery process can be started on the target replication server. Files are recovered only if all the following conditions are met:

- Version 7.1.1 or later, is installed on the source and target replication servers.
- The REPLRECOVERDAMAGED system parameter is set to ON. The system parameter can be set by using the SET REPLRECOVERDAMAGED command.
- The source server includes at least one file that is marked as damaged in the node that is being replicated.
- The node data was replicated before the damage occurred.

The following table describes how settings affect the recovery of damaged, replicated files.
Restriction: You cannot use the REPLRECOVERDAMAGED parameter for directory-container or cloud storage pools.

Table 1. Settings that affect the recovery of damaged files

Setting for the REPLRECOVERDAMAGED system parameter	**Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command**	**Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands**	**Result**
OFF	YES, NO, or not specified	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
OFF	ONLY	YES or NO	An error message is displayed because files cannot be recovered when the REPLRECOVERDAMAGED system parameter is set to OFF.
ON	YES	YES or NO	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	NO	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
ON	ONLY	YES or NO	Damaged files are recovered from the target replication server, but standard node replication does not occur.
ON	Not specified	YES	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	Not specified	NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.

Tip: When the QUERY PROCESS command is issued during node replication, the output can show unexpected results for the number of completed replications. The reason is that, for node replication purposes, each file space is considered to contain three logical file spaces:

- One for backup objects
- One for archive objects
- One for space-managed objects

By default, the QUERY PROCESS command generates results for each logical file space. Other factors also affect the output of the QUERY PROCESS command:

- If a file space has a replication rule that is set to NONE, the file space is not included in the count of file spaces that are being processed.
- If you specify data types in the REPLICATE NODE command, only those data types are included in the count of file spaces that are being processed, minus any file spaces that are excluded.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
   '-FORCEREConcile--=--+-No---+-'
                        +-Yes--+
                        '-FULL-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------+-------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (3) |
                        '-Fasp-----'
```

Notes:

1. Do not mix file space identifiers (FSIDs) and file space names in the same command.
2. Do not specify FSID if you use wildcard characters for the client node name.
3. Linux The TRANSFERMETHOD parameter is available only on Linux x86_64 operating systems.

Parameters

node_name or node_group_name (Required)
: Specifies the name of the client node or defined group of client nodes whose data is to be replicated. You can also specify a combination of client node names and client-node group names. To specify multiple client node names or client-node group names, separate the names with commas with no intervening spaces. You can use wildcard characters with client node names but not with client-node group names. The replication rules for all file spaces in the specified client nodes are checked.

filespace_name or FSID
: Specifies the name of the file space or the file space identifier (FSID) to be replicated. A name or FSID is optional. If you do not specify a name or an FSID, all the data in all the file spaces for the specified client nodes is eligible for replication.

  filespace_name
  : Specifies the name of the file space that has data to be replicated. File space names are case-sensitive. To determine the correct capitalization for the file space, issue the QUERY FILESPACE command. Separate multiple names with commas with no intervening spaces. When you specify a name, you can use wildcard characters.

    A server that has clients with file spaces that are enabled for Unicode might have to convert the file space name. For example, the server might have to convert a name from the server code page to Unicode. For details, see the NAMETYPE parameter. If you do not specify a file space name, or if you specify a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

  FSID
  : Specifies the file space identifier for the file space to be replicated. The server uses FSIDs to find the file spaces to replicate. To determine the FSID for a file space, issue the QUERY FILESPACE command. Separate multiple FSIDs with commas with no intervening spaces. If you specify an FSID, the value of the NAMETYPE parameter must be FSID.

NAMEType
: Specifies how you want the server to interpret the file space names that you enter. You can use this parameter for IBM Spectrum Protect™ clients that are enabled for Unicode and that have Windows, Macintosh OS X, or NetWare operating systems.
  Use this parameter only when you enter a partly qualified or fully qualified file space name. The default value is SERVER. You can specify one of the following values:

  SERVER
  : The server uses the server code page to interpret file space names.

  UNIcode
  : The server converts file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the characters in the name and the server code page. Conversion can fail if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines.

  FSID
  : The server interprets file space names by using their file space identifiers.

CODEType

Specifies the type of file spaces to be included in node replication processing. Use this parameter only when you enter a single wildcard character for the file space name. The default value is BOTH, which specifies that file spaces are included regardless of code page type. You can specify one of the following values:

UNIcode
: Specifies file spaces that are only in Unicode.

NONUNIcode
: Specifies file spaces that are not in Unicode.

BOTH
: Specifies all file spaces regardless of code page type.

DATAtype
: Specifies the type of data to be replicated. Data is replicated according to the replication rule that applies to the data type. This parameter is optional. You can specify one or more data types. If you do not specify a data type, all backup, archive, and space-managed data is replicated. Separate multiple data types with commas with no intervening spaces. You cannot use wildcard characters. You can specify one of the following values:

  ALl
  : Replicates all backup, archive, and space-managed data in a file space according to the rule that is assigned to the data type. For example, suppose that NODE1 has a single file space. The following replication rules apply:

    - The file space rules for backup and archive data in the file space are set to ALL_DATA.
    - The file space rule for space-managed data is set to DEFAULT.
    - The client node rule for space-managed data is set to NONE.

    If you issue `REPLICATE NODE NODE1 DATATYPE=ALL`, only backup data and archive data are replicated.

  BACKUP
  : Replicates active and inactive backup data in a file space if the controlling replication rule is ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY, or ACTIVE_DATA_HIGH_PRIORITY.

  BACKUPActive
  : Replicates only active backup data in a file space if the controlling replication rule is ACTIVE_DATA or ACTIVE_DATA_HIGH_PRIORITY.

  ARCHive
  : Replicates archive data only in a file space if the controlling replication rule is ALL_DATA or ALL_DATA_HIGH_PRIORITY.

  SPACEManaged
  : Replicates only space-managed data in a file space if the controlling replication rule is ALL_DATA or ALL_DATA_HIGH_PRIORITY.

PRIority
: Specifies the data to replicate based on the priority of the replication rule. You can specify one of the following values:

  All
  : Replicates all data in a file space if the controlling replication rule is ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY, or ACTIVE_DATA_HIGH_PRIORITY.

  High
  : Replicates only data in a file space that has a controlling replication rule of ALL_DATA_HIGH_PRIORITY or ACTIVE_DATA_HIGH_PRIORITY.

  Normal
  : Replicates only data in a file space that has a controlling replication rule of ALL_DATA or ACTIVE_DATA.

MAXSESSions
: Specifies the maximum allowable number of data sessions to use for sending data to a target replication server. This parameter is optional. The value can be 1 - 99. The default value is 10.

  Increasing the number of sessions can improve node replication throughput.

  When you set this value, consider the number of logical and physical drives that can be dedicated to the replication process. To access a sequential-access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on the following factors:

  - Other IBM Spectrum Protect and system activity
  - The mount limits of the device classes for the sequential access storage pools that are involved

Ensure that sufficient mount points and drives are available to allow node replication processes to complete. Each replication session might need a mount point on the source and target replication servers for storage pool volumes. If the device type is not FILE, each session might also need a drive on both the source and target replication servers.

When you set a value for MAXSESSIONS, also consider the available bandwidth and the processor capacity of the source and target replication servers.

Tip:

- The value that is specified by the MAXSESSIONS parameter applies only to data sessions. Data sessions are sessions during which data is sent to a target replication server. However, if you issue a QUERY SESSION command, the total number of sessions might exceed the number of data sessions. The difference is because of short control sessions that are used for querying and setting up replication operations.
- The value of the MAXSESSIONS parameter represents the maximum allowable number of sessions. The number of sessions that are used for replication depends on the amount of data to be replicated. If you are replicating only a small amount of data, you do not achieve any benefit by increasing the number of sessions. The total number of sessions might be less than the value that is specified by the MAXSESSIONS parameter.

Preview

Specifies whether to preview data. This parameter is optional. The default value is NO. You can specify one of the following values:

No

Specifies that the data is replicated to the target server but that the data is not previewed.

Yes

Specifies that data is previewed but not replicated. If you specify PREVIEW=YES, only volumes that must be physically mounted, such as tape volumes, are displayed. Volumes that are assigned to storage pools that have a device class of FILE are not displayed.

The following information is displayed in the output:

- The names of client nodes whose data would be replicated.
- The number of files that would be replicated or deleted.
- The estimated amount of time it would take to complete the node replication process.
- A list of volumes that would be mounted.
- A summary of information about replicated, damaged data. The summary lists the number of nodes, file spaces, files, and bytes that can be recovered during a replication recovery process. The summary is displayed only if RECOVERDAMAGED=YES or RECOVERDAMAGED=ONLY is specified.

If the client node data that is specified by the REPLICATE NODE command was never replicated and you specify `PREVIEW=YES`, the node and its file spaces are automatically defined on the target replication server.

LISTfiles

Specifies whether to list the names of files that would be replicated. This parameter is optional. The default is NO. Specifying this parameter signifies that the WAIT parameter is set to YES and that you cannot issue the WAIT parameter from the server console.

You can specify one of the following values:

No

Specifies that the names of files that would be replicated are not displayed.

Yes

Specifies that the names of files that would be replicated are displayed.

Wait

Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default value is NO. You can specify one of the following values:

No

Specifies that the command processes in the background. To monitor the background processing of the REPLICATE NODE command, issue the QUERY PROCESS command.

Yes

Specifies that the command processes in the foreground. Messages are not displayed until the command completes processing. You cannot specify `WAIT=YES` from the server console.

RECOVERDamaged
Specifies whether a recovery process is started on a target replication server after the node replication process is completed. This parameter is optional, and it overrides any value that you specified for the RECOVERDamaged parameter when you defined or updated a node. You can specify one of the following values:

Yes
Specifies that a replication process is started to recover damaged files, but only if the setting for the REPLRECOVERDAMAGED system parameter is ON. If the setting is OFF, damaged files are not recovered.

No
Specifies that damaged files are not recovered.

Only
Specifies that a replication process is started for the sole purpose of recovering damaged files, but only if the setting for the REPLRECOVERDAMAGED system parameter is ON. If the setting is OFF, damaged files are not recovered, and you receive a notification that recovery was not started.
Restriction: If you specify an invalid combination of values and settings for file recovery, replication is stopped, and an error message is displayed.

FORCEREConcile
Specifies whether to compare all files on the source replication server with files on the target replication server and to synchronize the differences between them. Before V7.1.1, this behavior was the default for replication processing. When IBM® Tivoli® Storage Manager V7.1.1 or later is installed on the source and target replication servers, a reconcile is automatically completed during initial replication. After initial replication, you might use this parameter for the following reasons:

- To synchronize files on the source and target replication servers if they are different.
- To replicate inactive files that were skipped after you change your replication rules from ACTIVE_DATA to ALL_DATA.
- To delete inactive files from the target replication server when you change your replication rules from ALL_DATA to ACTIVE_DATA.
- To ensure that you replicate only active data when you are using the ACTIVE_DATA replication rule so that the target replication server has active files only.
- To resynchronize the files so that the target replication server has the same files as the source replication server if you have previously or are currently using the policies on the target replication server to manage replicated files.
- To resynchronize the files on the source and target replication servers if the database is regressed to an earlier point-in-time by using a method other than the DSMSERV RESTORE DB command.
- To rebind files to the new management class on the target replication server if this management class did not exist when the files were replicated. You must be using the policies that are defined on the target replication server to manage replicated files.
- To remove all files on a target server for a node and file space that do not exist on the replication source server.

Remember: When the ACTIVE_DATA rule is assigned, a reconcile is completed only for active files on the source replication server.

This parameter is optional. You can specify one of the following values:

No
Specifies that replication processing does not force a reconcile to compare all files on the source replication server with files on the target replication server. Instead, replication processing tracks file changes on the source replication server since the last replication and synchronizes these changes on the target replication server. NO is the default value.

Yes
Specifies that replication processing forces a reconcile to compare all files on the source replication server with files on the target replication server and synchronizes the files on the target replication server with the source replication server.

FULL
Specifies that replication processing forces a reconcile to compare all files on the source replication server with files on the target replication server and synchronizes the files on the target replication server with the source replication server. Any files that do not exist on the source replication server are removed from the target replication server. Files might be removed for the following reasons:

- As a result of file space backup or import operations, files on the target replication server are no longer managed by replication processing.
- Replication-related orphaned objects on the target server are no longer managed by replication processing.

Restriction: Objects are deleted from the target replication server when nodes and file spaces are recognized by a replication process but the objects are not recognized.

Linux TRANSFERMethod

Linux Specifies the method that is used for server-to-server data transfer. This parameter is optional. You can specify one of the following values:

Tcpip
: Specifies that TCP/IP is used to transfer data. This value is the default.

Fasp
: Specifies that Aspera® Fast Adaptive Secure Protocol (FASP) technology is used to transfer data. Aspera FASP technology can help you optimize data transfer in a wide area network (WAN). If you specify TRANSFERMETHOD=FASP, you override any TRANSFERMETHOD parameters that you specified on the DEFINE SERVER or UPDATE SERVER commands.
Restrictions:

- Only data that is stored in a directory-container storage pool can be transferred by using Aspera FASP technology. Data that is not stored in a directory-container storage pool is transferred by using TCP/IP.
- Before you enable Aspera FASP technology, determine whether the technology is appropriate for your system environment and install the appropriate licenses. For instructions, see Determining whether Aspera FASP technology can optimize data transfer in your system environment. If the licenses are missing or expired, node replication fails.
- If WAN performance meets your business needs, do not enable Aspera FASP technology.

Example: Replicate data by data type and priority

Replicate high-priority active backup data and high-priority archive data that belongs to all the client nodes in group PAYROLL.

```
replicate node payroll datatype=backupactive,archive priority=high
```

Example: Replicate all the data that belongs to a node according to the assigned replication rules

NODE1 has a single file space. The following replication rules apply:

- File space rules:
  - Backup data: ACTIVE_DATA
  - Archive data: DEFAULT
  - Space-managed data: DEFAULT
- Client node rules:
  - Backup data: DEFAULT
  - Archive data: ALL_DATA_HIGH_PRIORITY
  - Space-managed data: DEFAULT
- Server rules:
  - Backup data: ALL_DATA
  - Archive data: ALL_DATA
  - Space-managed data: NONE

```
replicate node node1 priority=all
```

Active backup data in the file space is replicated with normal priority. Archive data is replicated with high priority. Space-managed data is not replicated.

Example: Recover damaged files without starting the full replication process

Without starting the full replication process, recover any damaged files in the client nodes of the PAYROLL group. Ensure that the setting for the REPLRECOVERDAMAGED system parameter is ON. Then, issue the following command:

```
replicate node payroll recoverdamaged=only
```

Related commands

Table 2. Commands related to REPLICATE NODE

Command	Description
CANCEL PROCESS	Cancels a background server process.
CANCEL REPLICATION	Cancels node replication processes.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLNODE	Displays information about the replication status of a client node.
QUERY REPLRULE	Displays information about node replication rules.
QUERY SERVER	Displays information about servers.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE REPLNODE	Removes a node from replication.
AIX Linux Windows PROTECT STGPOOL	Protects a directory-container storage pool.
SET REPLRECOVERDAMAGED	Specifies whether node replication is enabled to recover damaged files from a target replication server.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE NODE	Changes the attributes that are associated with a client node.
UPDATE REPLRULE	Enables or disables replication rules.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

REPLY (Allow a request to continue processing)

Use this command and an identification number to inform the server that you have completed a requested operation. Not all server requests require a reply. This command is required only if the request message specifically indicates that a reply is needed.

Privilege class

To issue this command, you must have system privilege or operator privilege.

Syntax

```
>>-REPly--request_number--+------------------------+-----------><
                          '-LABEL--=--volume_label-'
```

Parameters

request_number **(Required)**
: Specifies the identification number of the request.

LABEL
: Specifies the label to be written on a volume when you reply to a message from a LABEL LIBVOLUME command process. This parameter is optional.

Example: Reply to a request

Respond to a reply request using 3 as the request number.

```
reply 3
```

Related commands

Table 1. Commands related to REPLY

Command	Description
CANCEL REQUEST	Cancels pending volume mount requests.
QUERY REQUEST	Displays information about all pending mount requests.

RESET PASSEXP (Reset password expiration)

Use the RESET PASSEXP command to reset the password expiration period to the common expiration period for administrator and client node passwords. The RESET PASSEXP command does not apply to passwords that are stored on an LDAP directory server.

Restriction: You cannot reset the password expiration period to the common expiration period with the SET PASSEXP command.

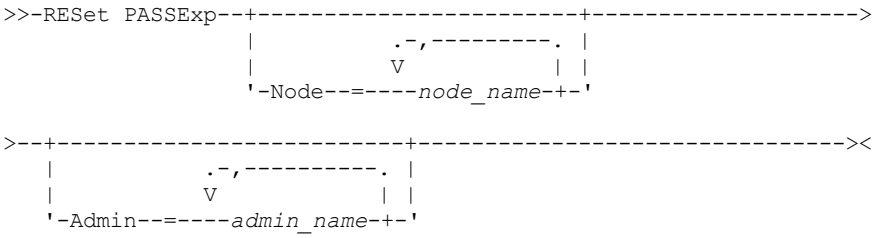
Use the QUERY STATUS command to display the common password expiration period.

Restriction: If you do not specify either the NODE or ADMIN parameters, the password expiration period for all client nodes and administrators will be reset.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

Node
: Specifies the name of the node whose password expiration period you would like to reset. To specify a list of nodes, separate the names with commas and no intervening spaces. This parameter is optional.

Admin
: Specifies the name of the administrator whose password expiration period you would like to reset. To specify a list of administrators, separate the names with commas and no intervening spaces. This parameter is optional.

Example: Reset the password expiration for specific client nodes

Reset the password expiration period for client nodes bj and katie.

```
reset passexp node=bj,katie
```

Example: Reset the password expiration for all users

Reset the password expiration period for all users to the common expiration period.

```
reset passexp
```

Related commands

Table 1. Commands related to RESET PASSEXP

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.
UPDATE NODE	Changes the attributes that are associated with a client node.

RESTART EXPORT (Restart a suspended export operation)

Use this command to restart a suspended export operation.

An export operation is suspended when any of the following conditions is detected:

- A SUSPEND EXPORT command is issued for the running export operation
- Segment preemption - the file being read for export is deleted by some other process
- Communication errors on a server-to-server export
- No available mount points
- Necessary volumes are unavailable
- I/O errors encountered

Important: Nodes or file spaces (on the exporting server) in the original export operation that are subsequently renamed are not included in the resumed operation. Any remaining data for nodes or file spaces on the target server that are deleted prior to resumption are discarded.

Privilege class

You must have system privilege to issue this command.

Syntax

```
                    .-*---------------------.
>>-RESTART EXPORT -+-----------------------+-------------------><
                    '---export_identifier---'
```

Parameters

export_identifier
: This optional parameter is the unique identifier for the suspended server-to-server export operation. You can use the wildcard character to specify this name. The export identifier name can be found by issuing the QUERY EXPORT command to list all the currently suspended server-to-server export operations.

Example: Restart a suspended export

Restart the suspended export operation identified by the export identifier EXPORTALLACCTNODES.

```
restart export exportallacctnodes
```

Related commands

Table 1. Commands related to RESTART EXPORT

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.

Command	Description
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
SUSPEND EXPORT	Suspends a running export operation.

RESTORE commands

Use the RESTORE commands to restore IBM Spectrum Protect™ storage pools or volumes.

- RESTORE NODE (Restore a NAS node)
- RESTORE STGPOOL (Restore storage pool data from a copy pool or an active-data pool)
- RESTORE VOLUME (Restore primary volume data from a copy pool or an active-data pool)

RESTORE NODE (Restore a NAS node)

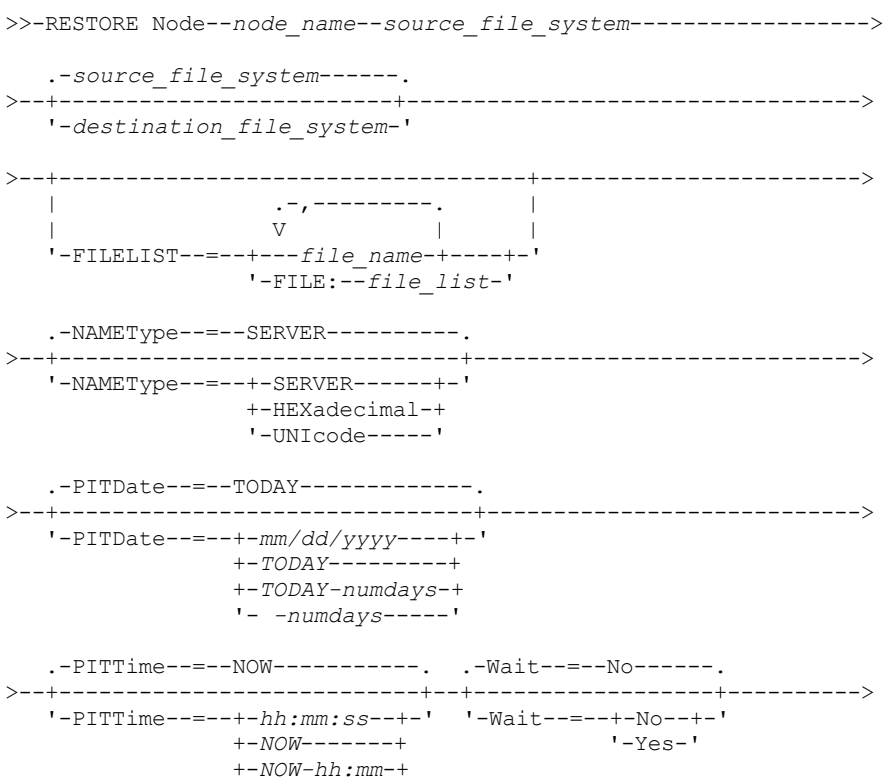
Use this command to initiate a restore operation for a network-attached storage (NAS) node.

You can use the RESTORE NODE command to restore backups that were created by using either the client's BACKUP NAS command or the server's BACKUP NODE command. NAS data may be restored from primary or copy native IBM Spectrum Protect™ pools; primary or copy NAS pools; or any combination needed to achieve the restore.

Privilege class

To issue this command, you must have system privilege, policy privilege for the domain to which the node is assigned, or client owner authority over the node.

Syntax



```
                '- -hh:mm---'

   .-TYPE--=--BACKUPImage-----.
>--+-------------------------+-------------------------------><
   '-TYPE--=--+-BACKUPImage-+-'
              '-SNAPMirror--'
```

Parameters

node_name (Required)
: Specifies the name of the node to restore. You cannot use wildcard characters or specify a list of names.

source_file_system (Required)
: Specifies the name of the file system to restore. You cannot use wildcard characters for this name. You cannot specify more than one file system to restore. Virtual file space names are allowed.

destination_file_system
: Specifies that the file server restores the data to an existing, mounted file system on the file server. This parameter is optional. The default is the original location of the file system on the file server. Virtual file space names are allowed.

FILELIST
: Specifies the list of file or directory names to be restored. This parameter is optional. The default is to restore the entire file system. If this value is specified, the server attempts to restore the objects from the appropriate image. If the PITDATE and PITTIME parameters are specified, then the file is restored from the last backup image prior to the specified time. If no PITDATE and PITTIME parameters are specified, the file is restored from the latest backup image of the file system.

  If the image is a differential backup, objects are first restored from the corresponding full backup and then from the differential backup. The restore is done by scanning the appropriate images for the specified objects and restoring any that are found. The TOCs for these images is not accessed, so the server does not check whether the objects are actually contained within the images.

  The folder path and file name must be entered using forward slash (/) symbols. No ending forward slash (/) is needed at the end of the file name. All arguments that contain a space must have double quotation marks ("argument with spaces") surrounding the entire argument.

  ```
  FILELIST="/path/to/filename1 with blanks",/path/to/filename2_no_blanks
  ```

  Any file names that contain commas must have double quotation marks surrounding the entire argument, surrounded by single quotation marks ('"argument with commas"').

  ```
  FILELIST='"/path/to/filename1,with,commas"',/path/to/filename2_no_commas
  ```

  To restore a complete directory, specify a directory name instead of a file name. All files in the directory and its subdirectories are restored. An ending forward slash (/) is not needed at the end of the directory name:

  ```
  FILELIST=/path/to/mydir
  ```

  file_name
  : Specifies one or more file or directory names to be restored. The names you specify cannot contain wildcards. Multiple names must be separated with commas and no intervening blanks. File names are case-sensitive.

  FILE:file_list
  : Specifies the name of a file that contains a list of the file or directory names to be restored. In the specified file, each file or directory name must be on a separate line. Blank lines and comment lines that begin with an asterisk are ignored. For example:
    To restore files FILE01, FILE02, and FILE03, create a file named RESTORELIST that contains a line for each file:

    ```
    FILE01
    FILE02
    FILE03
    ```

    You can specify the files to be restored with the command as follows:

    ```
    FILELIST=FILE:RESTORELIST
    ```

NAMEType
: Specifies how you want the server to interpret the names specified as FILELIST=file_name or the names listed in the file specified with FILELIST=file_list. This parameter is useful when the names may contain Unicode characters. It has no effect if the FILELIST parameter is not specified. The default value is SERVER. Possible values are:

SERVER
The server uses the server's code page to interpret the names.
HEXadecimal
The server interprets the names that you enter as the hexadecimal representation of a name in Unicode. To view the hexadecimal representation of a file or directory name, you can use the QUERY TOC command with FORMAT=DETAILED.
UNIcode
The server interprets the names as being UTF-8 encoded. This option only applies when you have specified a list with FILELIST=FILE:file_list.

Restriction: Network Data Management Protocol (NDMP) has limitations that prevent IBM Spectrum Protect from reporting whether or not individual files and directories are successfully restored.

PITDate
Specifies the point-in-time date. When used with the PITTIME parameter, PITDATE establishes the point in time from which you want to select the data to restore. The latest data that was backed up on or before the date and time that you specify will be restored. This parameter is optional. The default is TODAY.
You can specify the date by using one of the following values:

Value	Description	Example
MM/DD/YYYY	A specific date	06/25/2001
TODAY	The current date	TODAY
TODAY-days *or* -days	The current date minus days specified	TODAY–7 *or* –7. To restore data that was backed up a week ago, specify PITDATE=TODAY-7 or PITDATE=-7.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

PITTime
Specifies the point-in-time time. When used with the PITDATE parameter, PITTIME establishes the point in time from which you want to select the data to restore. The latest data that was backed up on or before the date and time that you specify will be restored. This parameter is optional. The default is the current time.
You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time on the specified date	12:33:28
NOW	The current time on the specified date	NOW
NOW-HH:MM *or* -HH:MM	The current time minus hours and minutes on the specified begin date	NOW-03:30 *or* -03:30. If you issue this command at 9:00 with PITTIME=NOW-03:30 or PITTIME=-03:30, the server restores backup records with a time of 5:30 or later on the point-in-time date.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. The default is NO. Possible values are:

No
Specifies that the server processes this command in the background. Use the QUERY PROCESS command to monitor the background processing of this command.
Yes

Specifies that the server processes this command in the foreground. You wait for the command to complete before continuing with other tasks. The server then displays the output messages to the administrative client when the command completes.
Restriction: You cannot specify WAIT=YES from the server console.

TYPE

Specifies the type of image to restore. The default value for this parameter is BACKUPIMAGE and it is used to restore data from standard NDMP base or differential backups. Other image types represent backup methods that might be specific to a particular file server. Possible values are:

BACKUPImage

Specifies that the file system should be restored from the appropriate standard NDMP backup images. This is the default method for performing an NDMP restore operation. Using the BACKUPIMAGE type, you can restore data from base and differential backups, and data at the file level.

SNAPMirror

Specifies that the file system should be retrieved from a NetApp SnapMirror image. SnapMirror images are block-level full-backup images of a NetApp file system. A SnapMirror image can only be restored to a file system that has been prepared as a SnapMirror target volume. Refer to the documentation that came with your NetApp file server for details.

After a SnapMirror image is retrieved and copied to a target file system, IBM Spectrum Protect breaks the SnapMirror relationship that was created by the file server during the operation. After the restore is complete, the target file system returns to the same state as that of the original file system at the point-in-time of the backup.

When setting the TYPE parameter to SNAPMIRROR, note the following restrictions:

Restrictions:

- You cannot specify the FILELIST parameter.
- Neither the *source_file_system_name* nor the *destination_file_system_name* can be a virtual filespace name.
- This parameter is valid for NetApp and IBM® N-Series file servers only.

Example: Restore a complete directory

Restore all of the files and subdirectories in the directory `/mydir`.

```
restore node nasnode /myfs /dest filelist=/path/to/mydir
```

Example: Restore data from a file system

Restore the data from the `/vol/vol10` file system on NAS node `NAS1`.

```
restore node nas1 /vol/vol10
```

Example: Restore a directory-level backup to the same location

Restore the directory-level backup to the original location. The source is the virtual file space name `/MIKESDIR` and no destination is specified.

```
restore node nas1 /mikesdir
```

For this example and the next example, assume the following virtual file space definitions exist on the server for the node `NAS1`.

```
VFS Name             Filesystem      Path
/mikesdir            /vol/vol2       /mikes
/TargetDirVol2       /vol/vol2       /tmp
/TargetDirVol1       /vol/vol1       /tmp
```

Example: Restore a directory-level backup to a different file system

Restore the directory-level backup to a different file system but preserve the path.

```
restore node nas1 /mikesdir /vol/vol0
```

Related commands

Table 1. Commands related to RESTORE NODE

Command	Description
BACKUP NODE	Backs up a network-attached storage (NAS) node.
CANCEL PROCESS	Cancels a background server process.
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
QUERY NASBACKUP	Displays information about NAS backup images.
QUERY TOC	Displays details about the table of contents for a specified backup image.

RESTORE STGPOOL (Restore storage pool data from a copy pool or an active-data pool)

Use this command to restore files from one or more copy storage pools or active-data pools to a primary storage pool.

IBM Spectrum Protect™ restores all the primary storage pool files that:

- Have been identified as having errors
- Reside on a volume with an access mode of DESTROYED

Restriction: You cannot use this command for container storage pools. Use the REPLICATE STGPOOL command to protect data for container storage pools.

You can also use this command to identify volumes that contain damaged, primary files. During restore processing, a message is issued for every volume in the restored storage pool that contains damaged, non-cached files. Use the QUERY CONTENT command to identify damaged, primary files on a specific volume.

You cannot restore a storage pool defined with a CENTERA device class.

In addition to restoring data to primary storage pools that have NATIVE or NONBLOCK data formats, this command also lets you restore data to primary storage pools that have NDMP data formats (NETAPPDUMP, CELERRADUMP, or NDMPDUMP). The primary storage pool must have the same data format as the copy storage pool from which data is to be restored. IBM Spectrum Protect supports backend data movement for NDMP images.

Tip: To restore NAS client-node data to NAS storage pools, you must manually change the access mode of the volumes to DESTROYED using the UPDATE VOLUME command. However, if you are using disaster recovery manager, the plan file will contain the information the server needs to automatically mark the volumes as DESTROYED.
Restoration of files might be incomplete if backup file copies in copy storage pools or active-data pools were moved or deleted by other IBM Spectrum Protect processes during restore processing. To prevent this problem, do not issue the following commands for copy storage pool or active-data pool volumes while restore processing is in progress:

- MOVE DATA
- DELETE VOLUME (DISCARDDATA=YES)
- AUDIT VOLUME (FIX=YES)

Also, you can prevent reclamation processing for your copy storage pools by setting the RECLAIM percentage to 100 with the UPDATE STGPOOL command.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the primary storage pool for which files are to be restored. If you are a restricted storage administrator and you want to restore files to a new primary storage pool, you must also have authority for the new storage pool.

Syntax

```
>>-RESTORE STGpool--primary_pool_name---------------------------->

>--+-------------------------------+-------------------------->
   '-COPYstgpool--=--copy_pool_name-'
```

```
   .-ACTIVEDATAOnly--=--No-------------.
>--+-----------------------------------+------------------------>
   '-ACTIVEDATAOnly--=--+-No---------+-'
                        '-Yes--| A |-'

>--+---------------------------------------+--------------------->
   '-NEWstgpool--=--new_primary_pool_name-'

   .-MAXPRocess--=--1------.  .-Preview--=--No------.
>--+----------------------+--+--------------------+----------->
   '-MAXPRocess--=--number-'  '-Preview--=--+-No--+-'
                                            '-Yes-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'

A (Yes)

|--ACTIVEDATAPool--=--active-data_pool_name--------------------|
```

Parameters

primary_pool_name (Required)
: Specifies the name of the primary storage pool that is being restored.

COPYstgpool
: Specifies the name of the copy storage pool from which the files are to be restored. This parameter is optional. If this parameter is not specified, files are restored from any copy pool in which copies can be located. Do not use this parameter with the ACTIVEDATAONLY or ACTIVEDATAPOOL parameters.

ACTIVEDATAOnly
: Specifies that active versions of backup files are to be restored from active-data pools only. This parameter is optional. The default is NO. If this parameter is not specified, files are restored from copy-storage pools. Do not use this parameter with the COPYSTGPOOL parameter. Possible values are:

  No
  : Specifies that the storage pool will not be restored from active-data pools.

  Yes
  : Specifies that the storage pool will be restored from active-pool or pools that you specify using the ACTIVEDATAPOOL parameter. If you specify YES as a value for ACTIVEDATAONLY, but do not specify a value for ACTIVEDATAPOOL, files are restored from any active-data pool in which active versions of backup files can be located.

  Attention: Restoring a primary storage pool from an active-data pool might cause some or all inactive files to be deleted from the database if the server determines that an inactive file needs to be replaced but cannot find it in the active-data pool.

ACTIVEDATAPool
: Specifies the name of the active-data pool from which the active versions of backup files are to be restored. This parameter is optional. If this parameter is not specified, files are restored from any active-data pool in which active versions of backup files can be located.

NEWstgpool
: Specifies the name of the new storage pool to which to restore the files. This parameter is optional. If this parameter is not specified, files are restored to the original primary storage pool (the pool being restored).

MAXPRocess
: Specifies the maximum number of parallel processes that are used for restoring files. Using multiple, parallel processes may improve throughput for the restore. This parameter is optional. You can specify a value from 1 to 999. The default is 1.

  When determining this value, consider the number of mount points (logical drives) and physical drives that can be dedicated to this operation. To access a sequential access volume, IBM Spectrum Protect uses a mount point, and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect and system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the restore.

Each process needs a mount point for copy storage pool volumes, and, if the device type is not FILE, each process also needs a drive. If you are restoring files in a sequential storage pool, each process needs an additional mount point for primary storage pool volumes and, if the device class is not FILE, an additional drive. For example, suppose you specify a maximum of 3 processes to restore a primary sequential storage pool from a copy storage pool of the same device class. Each process requires two mount points and two drives. To run all three processes, the device class must have a mount limit of at least 6, and at least 6 mount points and 6 drives must be available.

To preview a restore, only one process is used and no mount points or drives are needed.

Preview
Specifies if you want to preview but not perform the restore. The preview lets you identify volumes required to restore the storage pool. The preview displays:

- A list of primary storage pool volumes that contain damaged files.
- The number of files and the number of bytes to be restored, assuming that the access mode of the required copy storage pool volumes is READWRITE or READONLY when the restore operation is performed.
- A list of copy storage pool volumes containing files to be restored. These volumes must be mounted if you perform the restore.
- A list of any volumes containing files that cannot be restored.

Note: For only a list of offsite copy storage pool volumes to be mounted during a restore, change the access mode of the copy pool volumes to UNAVAILABLE. This prevents reclamation and move data processing of the volumes until they are moved onsite for the restore.
This parameter is optional. The default is NO. Possible values are:

No
Specifies that the restore is done.
Yes
Specifies that you want to preview the restore but not do the restore.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. Possible values are:

No
Specifies that the server processes this command in the background.

You can continue with other tasks while the command is being processed.

Messages created from the background process are displayed either in the activity log or the server console, depending on where messages are logged. To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files may have already been restored prior to the cancellation.

Yes
Specifies that the server performs this operation in the foreground. The operation must complete before you can continue with other tasks. The server then displays the output messages to the administrative client when the operation completes.
Note: You cannot specify WAIT=YES from the server console.

Example: Restore files from a copy storage pool to the primary storage pool

Restore files from any copy storage pool to the primary storage pool, PRIMARY_POOL.

```
restore stgpool primary_pool
```

Example: Restore files from a specific active-data pool to the primary storage pool

Restore files from active-data pool ADP1 to the primary storage pool PRIMARY_POOL.

```
restore stgpool primary_pool activedataonly=yes activedatapool=adp1
```

Related commands

Table 1. Commands related to RESTORE STGPOOL

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
CANCEL PROCESS	Cancels a background server process.
COPY ACTIVEDATA	Copies active backup data.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY PROCESS	Displays information about background processes.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
UPDATE STGPOOL	Changes the attributes of a storage pool.
UPDATE VOLUME	Updates the attributes of storage pool volumes.

RESTORE VOLUME (Restore primary volume data from a copy pool or an active-data pool)

Use this command to restore all files on damaged volumes in a primary storage pool that was backed up to a copy storage pool or copied to an active-data pool. IBM Spectrum Protect™ does not restore cached copies of files and removes those cached files from the database during restore processing.

In addition to restoring data to volumes in storage pools that have NATIVE or NONBLOCK data formats, this command also lets you restore data to volumes in storage pools that have NDMP data formats (NETAPPDUMP, CELERRADUMP, or NDMPDUMP). The volumes to be restored must have the same data format as the volumes in the copy storage pool. IBM Spectrum Protect supports backend data movement for NDMP images.

This command changes the access mode of the specified volumes to DESTROYED. When all files on a volume are restored to other locations, the destroyed volume is empty and is deleted from the database.

The restoration may be incomplete for one or more of the following reasons:

- Files were either never backed up or the backup copies are marked as damaged. Use the QUERY CONTENT command to get more information on the remaining files on the volume.
- A copy storage pool was specified on the RESTORE command, but files were backed up to a different copy storage pool. Use the PREVIEW parameter when you issue the RESTORE command again to determine if this is the problem.
- Volumes in the copy storage pool needed to perform the restore operation are offsite or unavailable. Check the activity log for messages that occurred during restore processing.
- Backup file copies in copy storage pools were moved or deleted by other processes during a restore. See note 3.
- An active-data pool was specified for the restore, and inactive files were not available to be copied.

Important:

1. You cannot restore volumes in storage pools defined with a CENTERA device class.
2. Before you restore a random-access volume, issue the VARY command to vary the volume offline.
3. To prevent copy storage pools files from being moved or deleted by other processes, do not issue the following commands for copy storage pool volumes during a restore:
   - MOVE DATA
   - DELETE VOLUME (DISCARDDATA=YES)
   - AUDIT VOLUME (FIX=YES)

   To prevent reclamation processing of copy storage pools, issue the UPDATE STGPOOL command with the RECLAIM parameter set to 100.

Privilege class

To issue this command you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the primary storage pool. If you have restricted privilege and want to restore files to a new primary storage pool, you must also have authority for the new storage pool.

Syntax

```
                  .-,-----------.
                  V             |
>>-RESTORE Volume----volume_name-+----------------------------->

>--+--------------------------------+-------------------------->
   '-COPYstgpool--=--copy_pool_name-'

   .-ACTIVEDATAOnly--=--No-------------.
>--+-----------------------------------+------------------------>
   '-ACTIVEDATAOnly--=--+-No---------+-'
                        '-Yes--| A |-'

>--+---------------------------------------+--------------------->
   '-NEWstgpool--=--new_primary_pool_name-'

   .-MAXPRocess--=--1------.  .-Preview--=--No------.
>--+----------------------+--+--------------------+----------->
   '-MAXPRocess--=--number-'  '-Preview--=--+-No--+-'
                                            '-Yes-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'

A (Yes)

|--ACTIVEDATAPool--=--active-data_pool_name--------------------|
```

Parameters

volume_name (Required)
: Specifies the name of the primary storage pool volume to be restored. To specify a list of volumes that belong to the same primary storage pool, separate the names with commas and no intervening spaces.

COPYstgpool
: Specifies the name of the copy storage pool from which the files are to be restored. This parameter is optional. If you do not specify this parameter, files are restored from any copy pool in which copies can be located. Do not use this parameter with the ACTIVEDATAONLY or ACTIVEDATAPOOL parameters.

ACTIVEDATAOnly
: Specifies that active versions of backup files are to be restored from active-data pools only. This parameter is optional. The default is NO. If this parameter is not specified, files are restored from copy-storage pools. Do not use this parameter with the COPYSTGPOOL parameter. Possible values are:

  No
  : Specifies that the storage pool will not be restored from active-data pools.

  Yes
  : Specifies that the storage pool will be restored from active-pool or pools that you specify using the ACTIVEDATAPOOL parameter. If you specify YES as a value for ACTIVEDATAONLY, but do not specify a value for ACTIVEDATAPOOL, files are restored from any active-data pool in which active versions of backup files can be located.

  Attention: Restoring a volume from an active-data pool might cause some or all inactive files to be deleted from the database if the server determines that an inactive file needs to be replaced but cannot find it in the active-data pool.

ACTIVEDATAPool
: Specifies the name of the active-data pool from which the active versions of backup files are to be restored. This parameter is optional. If this parameter is not specified, files are restored from any active-data pool in which active versions of backup files can be located.

NEWstgpool
: Specifies the name of the new storage pool to which to restore the files. This parameter is optional. If you do not specify this parameter, files are restored to the original primary storage pool.

MAXPRocess
: Specifies the maximum number of parallel processes to use for restoring files. Using parallel processes may improve throughput. This parameter is optional. You can specify a value from 1 to 999. The default is 1.

When determining this value, consider the number of mount points (logical drives) and physical drives that can be dedicated to this operation. To access a sequential access volume, IBM Spectrum Protect uses a mount point, and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect and system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the restore.

Each process needs a mount point for copy storage pool volumes. If the device type is not FILE, each process also needs a drive. If you are restoring a sequential storage pool, each process needs an additional mount point for primary storage pool volumes and, if the device type is not FILE, an additional drive. For example, suppose you specify a maximum of three processes to back up a primary sequential storage pool to a copy storage pool of the same device class. Each process requires two mount points and two drives. To run all three processes, the device class must have a mount limit of at least 6, and at least 6 mount points and 6 drives must be available.

To preview a backup, only one process is used and no mount points or drives are needed.

Preview
Specifies if you want to preview but not perform the restore. You can use this option to identify the offsite volumes required to restore a storage pool. This parameter is optional. The default is NO. Possible values are:

No
Specifies that you want to perform the restore operation.

Yes
Specifies that you want to preview the restore operation but restore the data.
Tip: If you preview a restore to see a list of offsite copy pool volumes to be mounted, you should you change the access mode of the identified volumes to UNAVAILABLE. This prevents reclamation and MOVE DATA processing for these volumes until they are transported to the onsite location for use in restore processing.
The preview displays the following:

- The number of files and bytes to be restored, if the access mode of the copy storage pool volumes is READWRITE or READONLY when the restoration is performed.
- A list of copy storage pool volumes containing files to be restored. These volumes must be mounted if you perform the restore.
- A list of volumes containing files that cannot be restored.

Wait
Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. This default is NO. Possible values are:

No
Specifies that the server processes this command in the background.

You can continue with other tasks while the command is being processed. Messages created from the background process are displayed either in the activity log or the server console, depending on where messages are logged.

To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files may have already been backed up prior to the cancellation.

Yes
Specifies that the server processes this command in the foreground. The operation must complete before you can continue with other tasks. The server then displays the output messages to the administrative client when the command completes.
Remember: You cannot specify WAIT=YES from the server console.

Example: Restore primary volume data files

Restore files stored on volume PVOL2 in primary storage pool PRIMARY_POOL.

```
restore volume pvol2
```

Example: Restore primary volume data files from an active-data pool

Restore files stored on volume VOL001 in primary pool PRIMARY_POOL from active-data pool ADP1.

```
restore volume vol001 activedataonly=yes activedatapool=adp1
```

Related commands

Table 1. Commands related to RESTORE VOLUME

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
COPY ACTIVEDATA	Copies active backup data.
CANCEL PROCESS	Cancels a background server process.
QUERY PROCESS	Displays information about background processes.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.

REVOKE commands

Use the REVOKE commands to revoke privileges or access.

- REVOKE AUTHORITY (Remove administrator authority)
- REVOKE PROXYNODE (Revoke proxy authority for a client node)

REVOKE AUTHORITY (Remove administrator authority)

Use this command to revoke one or more privilege classes from an administrator.

You can also use this command to reduce the number of policy domains to which a restricted policy administrator has authority and the number of storage pools to which a restricted storage administrator has authority.

If you use the REVOKE AUTHORITY command without the CLASSES, DOMAINS, and STGPOOLS parameters, you will revoke all privileges for the specified administrator.

At least one administrator must have system privilege; therefore, if the administrator is the only one with system privilege, you cannot revoke the authority.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-REVoke AUTHority--admin_name--------------------------------->

>--+-------------------------------------+---------------------->
   |                  .-,---------------. |
   |          (1)     V                 | |
   '-CLasses------=-----+-SYstem------+-+-'
                        +-Policy------+
                        +-STorage-----+
                        +-Operator----+
                        '-Node--| A |-'

>--+-----------------------------+----------------------------->
   |              .-,-----------. |
   |              V             | |
   '-DOmains--=-----domain_name-+-'

>--+---------------------------------+--------------------------><
   |                   .-,---------. |
   |           (1)     V           | |
   '-STGpools------=----pool_name-+-'

A

   .-AUTHority--=--Access-----.
```

```
|--+-------------------------+--+-DOmains--=--domain_name-+----|
   '-AUTHority--=--+-Access-+-'  '-NOde--=--node_name------'
                   '-Owner--'
```

Notes:

1. If all these parameters are omitted, all administrator privileges will be revoked for this administrator.

Parameters

admin_name (Required)
: Specifies the name of the administrator whose administrative privilege is to be revoked or reduced.

CLasses
: Specifies one or more administrative privilege classes to be revoked. You can specify more than one class by separating each with a comma.

  SYstem
  : Indicates that system authority is to be revoked for this administrator. If CLASSES=SYSTEM is specified, no other classes can be specified, and the DOMAINS and STGPOOLS parameters cannot be specified.

  Policy
  : Indicates that policy privilege is to be revoked for this administrator. To revoke all policy privilege, specify CLASSES=POLICY and do not specify the DOMAINS parameter.

  STorage
  : Indicates that storage privilege is to be revoked for this administrator. To revoke all storage privilege, specify CLASSES=STORAGE and do not specify the STGPOOLS parameter.

  Operator
  : Indicates that operator privilege is to be revoked for this administrator.

  Node
  : Indicates that node privilege is to be revoked for this user.

    AUTHority
    : Indicates the authority level to revoke for a user with node privilege. This parameter is optional.

      If an administrator already has system or policy privilege to the policy domain to which the node belongs, this command will not change the administrator's privilege.

      Possible authority levels are:

      Access
      : Indicates that client access authority is revoked. This is the default when CLASSES=NODE is specified. Note: A client node can set the REVOKEREMOTEACCESS option to prevent access by a user with node privilege and client access authority. If a user with node privilege has client owner authority, or has system or policy privileges to the policy domain to which the node belongs, that administrator can still access the web backup-archive client.

      Owner
      : Indicates that client owner authority is revoked.

    DOmains
    : Indicates that you want to revoke an administrator's client access or client owner authority to all clients in the specified policy domain. This parameter cannot be used together with the NODE parameter.

    NOde
    : Indicates that you want to revoke an administrator's client access or client owner authority to the node. This parameter cannot be used together with the DOMAIN parameter.

DOmains
: When used with CLASSES=POLICY, specifies a list of policy domains that can no longer be managed by a restricted policy administrator. (The administrator was authorized to manage these domains until the REVOKE command was issued.) This parameter is optional. The items in the list are separated by commas, with no intervening spaces. You can use wildcard characters to specify a name. Authority for all matching domains is revoked. If DOMAINS is specified, the parameter CLASSES=POLICY is optional.

STGpools
: Specifies a list of storage pools that can no longer be managed by a restricted policy administrator. (The administrator had been authorized to manage these storage pools until the REVOKE command was issued.) This parameter is optional. The items in the list are separated by commas, with no intervening spaces. You can use wildcard characters to specify a name.

Authority for all matching storage pools will be revoked. If STGPOOLS is specified then the parameter CLASSES=STORAGE is optional.

Usage notes

1. To change an unrestricted storage administrator to a restricted storage administrator, you must first use this command to revoke the unrestricted privilege. Then, use the GRANT AUTHORITY command to grant the administrator restricted storage privilege and to identify the storage pools to which the administrator has authority.

   To revoke unrestricted storage privilege from an administrator, specify the CLASSES=STORAGE parameter. You cannot use the STGPOOLS parameter to revoke authority for selected storage pools from an unrestricted storage administrator.

2. To change an unrestricted policy administrator to a restricted policy administrator, you must first use this command to revoke the unrestricted privilege. Then, use the GRANT AUTHORITY command to grant the administrator restricted policy privilege and to identify the policy domains to which the administrator has authority.

   To revoke unrestricted policy privilege from an administrator, specify the CLASSES=POLICY parameter. You cannot use the DOMAINS parameter to revoke authority for selected domains from an unrestricted administrator.

Example: Revoke certain administrative privileges

Revoke part of administrator CLAUDIA's privileges. CLAUDIA has restricted policy privilege for the policy domains EMPLOYEE_RECORDS and PROG1. Restrict CLAUDIA's policy privilege to the EMPLOYEE_RECORDS policy domain.

```
revoke authority claudia classes=policy
domains=employee_records
```

Example: Revoke all administrative privileges

Administrator LARRY currently has operator and restricted policy privilege. Revoke all administrative privileges for administrator LARRY. To revoke all administrative privileges for an administrator, identify the administrator, but do not specify CLASSES, DOMAINS, or STGPOOLS. LARRY remains an administrator but he can only use those commands that can be issued by any administrator.

```
revoke authority larry
```

Example: Revoke node privilege

Help desk personnel user CONNIE currently has node privilege with client owner authority for client node WARD3. Revoke her node privilege with client owner authority.

```
revoke authority connie classes=node
authority=owner node=ward3
```

Related commands

Table 1. Commands related to REVOKE AUTHORITY

Command	Description
GRANT AUTHORITY	Assigns privilege classes to an administrator.
QUERY ADMIN	Displays information about one or more IBM Spectrum ProtectIBM Spectrum Protect™ administrators.

REVOKE PROXYNODE (Revoke proxy authority for a client node)

Use this command to revoke authority for an agent client node to perform backup and restore operations for a target node on the IBM Spectrum Protect™ server.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege

Syntax

```
>>-REVoke PROXynode TArget--=--target_node_name----------------->

>--AGent--=--agent_node_name----------------------------------><
```

Parameters

TArget (Required)
: Specifies the target node to which an agent node has been granted proxy authority. Wildcard characters and comma-separated lists of node names are allowed.

AGent (Required)
: Specifies which node has authority to act as proxy to the target node. Wildcard characters and comma-separated lists of node names are allowed.

Example: Revoke a node's proxy authority

To revoke authority from target node NASCLUSTER to act as proxy for all agent nodes which start with the letter M, issue the following command.

```
revoke proxynode target=nascluster agent=m*
```

Related commands

Table 1. Commands related to REVOKE PROXYNODE

Command	Description
GRANT PROXYNODE	Grant proxy authority to an agent node.
QUERY PROXYNODE	Display nodes with authority to act as proxy nodes.

ROLLBACK (Rollback uncommitted changes in a macro)

Use this command within a macro to undo any processing changes made by commands run by the server but not yet committed to the database. A committed change is permanent and cannot be rolled back. The ROLLBACK command is useful for testing macros.

Ensure that your administrative client session is not running with the ITEMCOMMIT option when using this command.

Important: SETOPT commands inside a macro cannot be rolled back.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-ROLLBACK--------------------------------------------------><
```

Parameters

None

Example: Rollback changes in a macro

Run the REGN macro with the ROLLBACK command to verify that the macro works without committing any changes. The macro contents are:

```
/* Macro to register policy
administrators and grant authority */
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
ROLLBACK  /* prevents any changes from being committed */
```

Related commands

Table 1. Commands related to ROLLBACK

Command	Description
COMMIT	Makes changes to the database permanent.
MACRO	Runs a specified macro file.

Related concepts:
Administrative client macros

RUN (Run an IBM Spectrum Protect script)

Use this command to run an IBM Spectrum Protect™ script. To issue this command on another server, the script being run must be defined on that server.

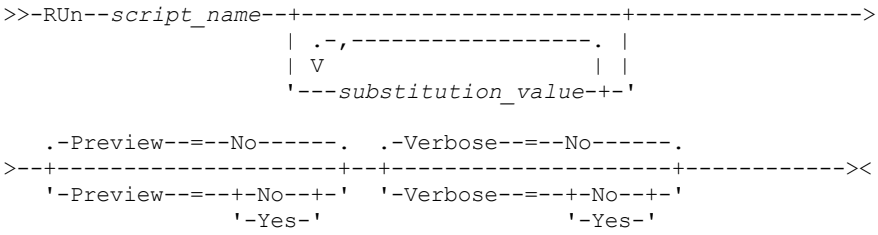
You can include RUN commands in scripts as long as they do not create loops. For example, you should avoid including RUN commands where SCRIPT_A runs SCRIPT_B and SCRIPT_B runs SCRIPT_A.

Important: IBM Spectrum Protect does not have a command that can cancel a script after it starts. To stop a script, you must halt the server.

Privilege class

To issue this command, you must have operator, policy, system, storage, or system privilege.

Syntax



Parameters

script_name (Required)
: Specifies the name of the script you want processed. The name you specify cannot be a substitution variable, such as $1.

substitution_value
: Specifies one or more values to substitute for variables when the script is run. In a script, a substitution variable consists of a '$' character, followed by a number. When you run the script, IBM Spectrum Protect replaces the substitution variables defined in a script with the values you supply with this command. You must specify values for each substitution variable defined in the script or the script will fail. This parameter is optional.

Preview
: Specifies whether to preview the command lines of a script without actually processing the script. The default is NO. Possible values are:

  Yes
  : Specifies that the command lines included in a script are displayed, but the script is not processed.

  No
  : Specifies that the command lines included in a script are displayed and the script is processed.

Verbose
: Specifies whether command lines, variable substitution, and conditional logic testing used in a script are displayed as the script is being processed. This parameter is ignored if PREVIEW=YES is specified. The default is NO.
Possible values are:

Yes
: Specifies that the command lines, variable substitution, and conditional logic testing are displayed as the script is being processed.

No
: Specifies that the command lines, variable substitution, and conditional logic testing do not display as the script is being processed.

Example: View the commands generated by a script with a table name substitution variable

To run the following example script, called QSAMPLE, you issue a RUN command that specifies the table name ACTLOG as the value for the substitution variable, $1. Use the output to preview the commands generated by the script before running the commands.

```
001  /* This is a sample SQL Query in wide format */
005  SET SQLDISPLAYMODE WIDE
010  SELECT colname FROM -
015  COLUMNS WHERE TABNAME='$1'

run qsample actlog preview=yes

ANR1461I RUN: Executing command script QSAMPLE.
ANR1466I RUN: Command script QSAMPLE, Line 5 :
              set sqldisplaymode wide.
ANR1466I RUN: Command script QSAMPLE, Line 15 :
              select colname from columns where tabname='ACTLOG'.
ANR1470I RUN: Command script QSAMPLE completed successfully
              (PREVIEW mode)
```

Example: Run a script to display and run the commands generated by the script

Run the same script as show in the prior example to display both the generated commands and the results of the commands.

```
run qsample actlog verbose=yes

ANR1461I RUN: Executing command script QSAMPLE.
ANR1466I RUN: Command script QSAMPLE, Line 5 :
              set sqldisplaymode wide.
ANR1466I RUN: Command script QSAMPLE, Line 5 : RC=RC_OK
ANR1466I RUN: Command script QSAMPLE, Line 15 :
              select colname from columns where tabname='ACTLOG'.

COLNAME
------------------
DATE_TIME
MSGNO
SEVERITY
MESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Command script QSAMPLE, Line 15 : RC=RC_OK
ANR1462I RUN: Command script QSAMPLE completed successfully.
```

Example: Run a script to display just the results of the commands in the script

Run the previous example script, without displaying just the results of the generated commands in the script.

```
run qsample actlog verbose=no

COLNAME
------------------
```

```
DATE_TIME
MSGNO
SEVERITY
MESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Command script QSAMPLE completed successfully.
```

Related commands

Table 1. Commands related to RUN

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
QUERY SCRIPT	Displays information about scripts.
RENAME SCRIPT	Renames a script to a new name.
UPDATE SCRIPT	Changes or adds lines to a script.

Related tasks:
Running a server script

SELECT (Perform an SQL query of the IBM Spectrum Protect database)

Use the SELECT command to create and format a customized query of the IBM Spectrum Protect™ database.

IBM Spectrum Protect provides an SQL interface to a DB2® program. Restrictions and guidelines for handling SQL queries are handled directly by DB2.

To help you find what information is available, IBM Spectrum Protect provides three system catalog tables:

SYSCAT.TABLES
: Contains information about all tables that can be queried with the SELECT command.

SYSCAT.COLUMNS
: Describes the columns in each table.

You can issue the SELECT command to query these tables to determine the location of the information that you want.

Usage notes

You cannot issue the SELECT command from a server console.

Because the select command does not lock and unlock records, contention for a record can cause the server to erroneously issue message ANR2034E: `SELECT: No match found using this criteria.` Check your selection criteria, and if you believe that it is correct, try the command again.

To stop the processing of a SELECT command after it starts, cancel the administrative session from which the command was issued. Cancel the session from either the server console or another administrative session.

Temporary table spaces are used to process SQL queries within DB2. Inadequate temporary space can cause SQL queries to fail.

To export output to a comma-separated file for import into a spreadsheet, use -comma and > command-line options on the dsmadmc command.

Privilege class

Any administrator can issue this command.

Syntax

For SELECT statement syntax and guidelines, search the DB2 product information.

Important: The appropriate syntax for the timestamp Select statement is:

```
SELECT * FROM SUMMARY WHERE ACTIVTY='EXPIRATION' AND START_TIME >'2009-05-10 00:00:00' AND
START_TIME <'2009-05-11 23:23:23'
```

List of examples

The SELECT command is used to customize a wide variety of queries. To give you an idea of what you can do with the command, this section includes many examples. There are, however, many more possibilities. Query output is shown only for the more complex commands to illustrate formatting.

The following list summarizes the example SELECT commands:

- List administrator user ID passwords that are authenticated with an external LDAP directory server
- List available tables
- List client nodes and administrative clients that are currently locked from server access
- List client nodes and administrative clients that have not specified the correct password lately
- List nodes in the standard policy domain that are not associated with the daily backup schedule DAILYBACKUP
- List the administrators that have policy authority
- List type E (ERROR) or W (WARNING) messages that have been issued in the time period for which activity log records have been maintained
- List the administrative schedules that have been defined or altered by administrator JAKE
- List the relative administrative schedule priorities
- List the management classes that have an archive copy group with a retention period greater than 365 days
- List the client nodes that are in each policy domain
- Count how many files have been archived from each node
- List the clients that are using space management
- Determine how many volumes would be reclaimed if the reclamation threshold is changed to 50 percent for storage pool TAPE
- Determine how many backup files would be affected for each node if the DAILY management class in the STANDARD policy domain is changed or deleted
- For all active client sessions, determine how long have they been connected and their effective throughput in bytes per second
- Determine how long the current background processes have been running and determine their effective throughput in time and files per second
- Count the number of client nodes are there for each platform type
- Count the number of file spaces each client node has and list the client nodes ascending order
- Obtain statistical information for calculating the number of off-site volumes that have their space reclaimed during reclamation of a storage pool
- Obtain PVU estimate detail records
- Obtain information about the node roles
- Obtain information about status

Example: List administrator user IDs that authenticate to the IBM Spectrum Protect server

List all the administrator user IDs whose passwords authenticate with the IBM Spectrum Protect server:

```
select admin_name from admins where
authentication=local
```

Example: List available tables

List all the tables available for querying the IBM Spectrum Protect database.

```
select * from syscat.tables

      ABSCHEMA: SERVER1
       TABNAME: ACTLOG
   CREATE_TIME: 1999-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 1
```

```
  UNIQUE_INDEX: FALSE
       REMARKS: Server activity log

     TABSCHEMA: SERVER1
       TABNAME: ADMIN_SCHEDULES
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 14
INDEX_COLCOUNT: 1
  UNIQUE_INDEX: TRUE
       REMARKS: Administrative command schedules

     TABSCHEMA: SERVER1
       TABNAME: ADMINS
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 15
INDEX_COLCOUNT: 1
  UNIQUE_INDEX: TRUE
       REMARKS: Server administrators

     TABSCHEMA: SERVER1
       TABNAME: ARCHIVES
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 5
  UNIQUE_INDEX: FALSE
       REMARKS: Client archive files
```

Example: List client nodes and administrative clients that are currently locked from server access

```
select node_name from nodes where locked='YES'

select admin_name from admins where locked='YES'
```

Example: List client nodes, administrative clients, and servers that are using transitional session security

```
select node_name from nodes where session_security='Transitional'

select admin_name from admins where session_security='Transitional'

select server_name from servers where session_security='Transitional'
```

Example: List client nodes and administrative clients that have not specified the correct password lately

```
select node_name from nodes where invalid_pw_count <>0

select admin_name from admins where invalid_pw_count <>0
```

Example: List nodes in the standard policy domain that are not associated with the daily backup schedule DAILYBACKUP

```
select node_name from nodes where domain_name='STANDARD' and
node_name not in (select node_name from associations
where domain_name='STANDARD' and
schedule_name='DAILYBACKUP')
```

Example: List the administrators who have policy authority

```
select admin_name from admins where
upper(system_priv) <>'NO'
or upper(policy_priv) <>'NO'
```

Example: List type E (ERROR) or W (WARNING) messages that have been issued in the time period for which activity log records have been maintained

```
select date_time,msgno,message from actlog
where severity='E' or severity='W'
```

Example: List the administrative schedules that have been defined or altered by administrator JAKE

```
select schedule_name from admin_schedules
where chg_admin='JAKE'
```

Example: List the relative administrative schedule priorities

```
select schedule_name,priority from admin_schedules order
by priority
```

Example: List the management classes that have an archive copy group with a retention period greater than 365 days

```
select domain_name,set_name,class_name from ar_copygroups
where retver='NOLIMIT' or cast(retver as integer) >365
```

Example: List the management classes that specify more than five backup versions

```
select domain_name,set_name,class_name from bu_copygroups
where verexists ='NOLIMIT' or
cast(verexists as integer)>5
```

Example: List the client nodes that are using the client option set named SECURE

```
select node_name from nodes where option_set='SECURE'
```

Example: List the client nodes that are in each policy domain

```
select domain_name,num_nodes from domains
```

Example: Count how many files have been archived from each node

Attention: This command might take a long time to complete.

```
select node_name,count(*) from archives
group by node_name
```

Example: List the clients that are using space management

```
select node_name from auditocc where spacemg_mb <>0
```

Example: Determine how many volumes would be reclaimed if the reclamation threshold is changed to 50 percent for storage pool TAPE

```
select count(*) from volumes where stgpool_name='TAPE'
and upper(status)='FULL' and pct_utilized < 50
```

Example: Determine how many backup files would be affected for each node if the DAILY management class in the STANDARD policy domain is changed or deleted

Note: This command takes significant time and resources to complete.

```
select node_name, count(*) as "Files" from backups
where class_name='DAILY' and node_name in
(select node_name from nodes where domain_name='STANDARD')
group by node_name
```

Example: For all active client sessions, determine how long have they been connected and their effective throughput in bytes per second

```
select session_id as "Session",
client_name as "Client",
state as "State",
current_timestamp-start_time as "Elapsed Time",
(cast(bytes_sent as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes sent/second",
(cast(bytes_received as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes received/second"
from sessions
```

```
                Session: 24
                 Client: ALBERT
                  State: Run
           Elapsed Time: 0 01:14:05.000000
      Bytes sent/second: 564321.9302768451
  Bytes received/second: 0.0026748857944

                Session: 26
                 Client: MILTON
                  State: Run
           Elapsed Time: 0 00:06:13.000000
      Bytes sent/second: 1638.5284210992221
  Bytes received/second: 675821.6888561849
```

Example: Determine how long the current background processes have been running and determine their effective throughput in time and files per second

Note: Expiration does not report the number of bytes processed.

```
select process_num as "Number",
process,
current_timestamp-start_time as "Elapsed Time",
(cast(files_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Files/second",
(cast(bytes_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes/second"
from processes
```

```
         Number: 1
        PROCESS: Expiration
   Elapsed Time: 0 00:24:36.000000
   Files/second: 6.3216755870092
   Bytes/second: 0.0000000000000
```

Example: Count the number of client nodes for each platform type

```
select platform_name,count(*) as "Number of Nodes"
from nodes group by platform_name
```

```
PLATFORM_NAME     Number of Nodes
-------------     ---------------

  AIX                   6
  SunOS                27
  Win32                14
  Linux                20
```

Example: Count the number of file spaces each client node has and list the client nodes ascending order

```
select node_name, count(*) as "number of filespaces"
from filespaces group by node_name order by 2
```

```
NODE_NAME              number of filespaces
------------------     --------------------
```

```
ALBERT                    2
MILTON                    2
BARNEY                    3
SEBASTIAN                 3
MAILHOST                  4
FALCON                    4
WILBER                    4
NEWTON                    4
JEREMY                    4
WATSON                    5
RUSSELL                   5
```

Example: Obtain statistical information for calculating the number of off-site volumes that have their space reclaimed during reclamation of a storage pool.

```
select * from summary where activity='OFFSITE RECLAMATION'

           START_TIME: 2004-06-16 13:47:31.000000
             END_TIME: 2004-06-16 13:47:34.000000
             ACTIVITY: OFFSITE RECLAMATION
               NUMBER: 4
               ENTITY: COPYPOOL
             COMMMETH:
              ADDRESS:
        SCHEDULE_NAME:
             EXAMINED: 170
             AFFECTED: 170
               FAILED: 0
                BYTES: 17821251
                 IDLE: 0
               MEDIAW: 0
           PROCESSES: 2
          SUCCESSFUL: YES
         VOLUME_NAME:
          DRIVE_NAME:
        LIBRARY_NAME:
            LAST_USE:
           COMM_WAIT:
    NUM_OFFSITE_VOLS: 2
```

Example: Identify which storage pools contain data that was deduplicated by clients

```
select stgpool_name,has_client_dedup_data from stgpools

STGPOOL_NAME                HAS_CLIENT_DEDUP_DATA
--------------------        --------------------
ADPOOL                      NO
ARCHIVEPOOL                 NO
BACKUPPOOL                  NO
COPYDEDUP                   NO
COPYNODEDUP                 NO
FILEPOOL                    YES
FILEPOOL2                   NO
LANFREEFILEPOOL             YES
SPACEMGPOOL                 NO
```

Example: Obtain information about the database

```
select * from db

       DATABASE_NAME: TSMDB1
  TOT_FILE_SYSTEM_MB: 2048000
    USED_DB_SPACE_MB: 12576
       FREE_SPACE_MB: 1576871
         TOTAL_PAGES: 983044
        USABLE_PAGES: 982908
          USED_PAGES: 977736
          FREE_PAGES: 5172
      BUFF_HIT_RATIO: 96.2
      TOTAL_BUFF_REQ: 53967
       SORT_OVERFLOW: 0
```

```
     LOCK_ESCALATION: 0
       PKG_HIT_RATIO: 70.0
           LAST_REORG: 2010-07-15 17:32:55.000000
      FULL_DEV_CLASS: OUTFILE
     NUM_BACKUP_INCR: 0
    LAST_BACKUP_DATE: 2010-01-21 10:37:59.000000
    PHYSICAL_VOLUMES: 0
           PAGE_SIZE:
  NUM_BACKUP_STREAMS: 4
```

Example: Obtain PVU estimate detail records

Generate the PVU estimate for a node named ACCTSRECSRV, which is used by the IBM Spectrum Protect Extended Edition product.

```
select * from pvuestimate_details where node_name='ACCTSRECSRV'
```

```
            PRODUCT: PRODEE
       LICENSE_NAME: MGSYSLAN
          NODE_NAME: ACCTSRECSRV
          LAST_USED: 2008-01-20 16:12:24.000000
             TRYBUY: FALSE
        PROC_VENDOR: IBM
         PROC_BRAND: POWER5+ QCM
          PROC_TYPE: 4
         PROC_MODEL:
         PROC_COUNT: 2
               ROLE: SERVER
      ROLE_OVERRIDE: USEREPORTED
    ROLE_EFFECTIVE: SERVER
       VALUE_UNITS: 50
  VALUE_FROM_TABLE: YES
                PVU: 100
       SCAN_ERROR : NO
        API_CLIENT: NO
      PVU_AGNOSTIC: NO
        HYPERVISOR: VMWARE
              GUID: 01.2e.1c.80.e5.04-
                     .11.da.aa.ab.00.-
                     15.58.0b.d9.47
           VERSION: 6
           RELEASE: 3
             LEVEL: 1
          VENDOR_D: IBM(R)
           BRAND_D: POWER5(TM) QCM
            TYPE_D: Quad-core Module
           MODEL_D: All Existing
        PRODUCT_D: IBM Spectrum Protect Extended Edition
```

Field descriptions

PRODUCT
: Rollup of license types into products at the level presented in the QUERY PVUESTIMATE command. Possible values are PRODEE, PROTBASIC, PRODDATARET, PRODMAIL, PRODDB, PRODSYSB, PRODSPACE, PRODSAN, PRODERP, or blank.

LICENSE_NAME
: The license assigned to this node.

NODE_NAME
: The node name.

LAST_USED
: Date and time the identified node last connected to the system under this license.

TRYBUY
: Indicates if running under try and buy mode. Possible values are TRUE or FALSE.

PROC_VENDOR
: Processor vendor name as reported by the client.

PROC_BRAND
: Processor brand name as reported by the client.

PROC_TYPE
: Processor type as reported by the client. This value also reflects the number of cores. Example values are 1=SINGLE CORE, 2=DUO CORE, and 4=QUAD CORE.

PROC_MODEL
: Processor model as reported by the client.

PROC_COUNT
: Processor quantity.

ROLE
: Node role. Possible values are CLIENT, SERVER, or OTHER.

ROLE_OVERRIDE
: Override value specified in the UPDATE NODE command.

ROLE_EFFECTIVE
: Actual role based on the values in the ROLE and ROLE_OVERRIDE fields.

VALUE_UNITS
: Assigned processor value unit (PVU) for the processor.

PVU
: Calculated PVU value.

```
PVU per node = number of processors per node * processor type * pvu value
```

where the `processor type` represents the number of cores, and the `pvu value` is the value defined for the processor type in the IBM® PVU table.

VALUE_FROM_TABLE
: Flag that indicates whether the PVU was calculated based on the IBM PVU table. Possible values are YES or NO. If NO, a value of 100 is applied for each node defined as a server. If no role is defined for a node, the role of server is assumed for purposes of PVU calculation.

SCAN_ERROR
: Flag that indicates whether license information was reported by client. Possible values are YES or NO.

API_CLIENT
: Flag that indicates an API application. Possible values are YES or NO.

PVU_AGNOSTIC
: Flag indicating that the client version release level is earlier than IBM Spectrum Protect V6.3. If the version is earlier than 6.3, valid PVU metrics are not expected. Possible values are YES or NO.

HYPERVISOR
: Name of the virtual machine software as reported by the client.

GUID
: Globally Unique Identifier (GUID) of the computer where the node is located. The GUID is obtained from the node table.

VERSION
: Version of client.

RELEASE
: Release of client.

LEVEL
: Level of client.

VENDOR_D
: Processor vendor display value from the PVU table.

BRAND_D
: Processor brand display value from the PVU table.

TYPE_D
: Processor type display value from the PVU table.

MODEL_D
: Processor model display value from the PVU table.

PRODUCT_D
: Product display value from the PVU table. The following values are possible:

  - IBM Spectrum Protect
  - IBM Spectrum Protect Extended Edition
  - IBM Spectrum Protect for Data Retention
  - IBM Spectrum Protect for SAN
  - IBM Spectrum Protect for Space Management
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for System Backup and Recovery
  - Blank

Example: Obtain role and PVU-related information

The following example shows partial results for a selected node, including PVU-related information and role information. Possible roles are CLIENT, SERVER, or OTHER. PVU is calculated only for nodes defined as servers.

```
select * from nodes

  ROLE: CLIENT
      ROLE_O: USEREPORTED
     PVENDOR: INTEL
      PBRAND: INTEL
       PTYPE: 4
      PMODEL:
      PCOUNT: 1
  HYPERVISOR:
        PAPI: NO
   SCANERROR: NO
```

SET commands

Use the SET commands to specify values that affect many different IBM Spectrum Protect™ operations.

- SET ACCOUNTING (Set accounting records on or off)
- SET ACTLOGRETENTION (Set the retention period or the size of the activity log)
- SET ALERTACTIVEDURATION (Set the duration of an active alert)
- SET ALERTCLOSEDDURATION (Set the duration of a closed alert)
- SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)
- SET ALERTEMAILFROMADDR (Set the email address of the sender)
- SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)
- SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)
- SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)
- SET ALERTMONITOR (Set the alert monitor to on or off)
- SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)
- SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)
- SET ARCHIVERETENTIONPROTECTION (Activate data retention protection)
- SET ARREPLRULEDEFAULT (Set the server replication rule for archive data)
- SET BKREPLRULEDEFAULT (Set the server replication rule for backup data)
- SET CLIENTACTDURATION (Set the duration period for the client action)
- SET CONFIGMANAGER (Specify a configuration manager)
- SET CONFIGREFRESH (Set managed server configuration refresh)
- SET CONTEXTMESSAGING (Set message context reporting on or off)
- SET CPUINFOREFRESH (Refresh interval for the client workstation information scan)
- SET CROSSDEFINE (Specifies whether to cross-define servers)
- SET DBRECOVERY (Set the device class for automatic backups)
- SET DEDUPVERIFICATIONLEVEL (Set the percentage of extents to verify)
- SET DEFAULTAUTHENTICATION (Set the default authentication method for REGISTER NODE and REGISTER ADMIN commands)
- SET DEPLOYPKGMGR (Enable the deployment package manager)
- SET DEPLOYREPOSITORY (Set the download path for client deployment packages)
- SET DEPLOYMAXPKGS (Set the maximum number of client deployment packages to store)
- SET DISSIMILARPOLICIES (Enable the policies on the target replication server to manage replicated data)
- SET DRMACTIVEDATASTGPOOL (Specify the active-data pools to be managed by DRM)
- SET DRMCHECKLABEL (Specify label checking)
- SET DRMCMDFILENAME (Specify the name of a file to contain commands)
- AIX Linux Windows SET DRMCOPYCONTAINERSTGPOOL (Specify the container-copy storage pools to be processed by DRM commands)
- SET DRMCOPYSTGPOOL (Specify the copy storage pools to be managed by DRM)
- SET DRMCOURIERNAME (Specify the courier name)
- SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)
- SET DRMFILEPROCESS (Specify file processing)
- SET DRMINSTRPREFIX (Specify the prefix for recovery instructions file names)
- SET DRMNOTMOUNTABLENAME (Specify the not mountable location name)
- SET DRMPLANPREFIX (Specify a prefix for recovery plan file names)

- SET DRMPLANVPOSTFIX (Specify replacement volume names)
- SET DRMPRIMSTGPOOL (Specify the primary storage pools to be managed by DRM)
- SET DRMRPFEXPIREDAYS (Set criteria for recovery plan file expiration)
- SET DRMVAULTNAME (Specify the vault name)
- SET EVENTRETENTION (Set the retention period for event records)
- SET FAILOVERHLADDRESS (Set a failover high level address)
- SET INVALIDPWLIMIT (Set the number of invalid logon attempts)
- SET LDAPPASSWORD (Set the LDAP password for the server)
- SET LDAPUSER (Specify an ID for an LDAP directory server)
- SET LICENSEAUDITPERIOD (Set license audit period)
- SET MAXCMDRETRIES (Set the maximum number of command retries)
- SET MAXSCHEDSESSIONS (Set maximum scheduled sessions)
- SET MINPWLENGTH (Set minimum password length)
- SET MONITORINGADMIN (Set the name of the monitoring administrator)
- SET MONITOREDSERVERGROUP (Set the group of monitored servers)
- SET NODEATRISKINTERVAL (Specifies at-risk mode for an individual node)
- SET PASSEXP (Set password expiration date)
- SET PRODUCTOFFERING (Set the product offering that is licensed to your enterprise)
- SET QUERYSCHEDPERIOD (Set query period for polling client nodes)
- SET RANDOMIZE (Set randomization of scheduled start times)
- SET REPLRECOVERDAMAGED (Specify whether damaged files are recovered from a replication server)
- SET REPLRETENTION (Set the retention period for replication records)
- SET REPLSERVER (Set the target replication server)
- SET RETRYPERIOD (Set time between retry attempts)
- SET SCHEDMODES (Select a central scheduling mode)
- SET SERVERHLADDRESS (Set the high-level address of a server)
- SET SERVERLLADDRESS (Set the low-level address of a server)
- SET SERVERNAME (Specify the server name)
- SET SERVERPASSWORD (Set password for server)
- SET SPREPLRULEDEFAULT (Set the server replication rule for space-managed data)
- SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)
- SET STATUSMONITOR (Specifies whether to enable status monitoring)
- SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)
- SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)
- SET SUBFILE (Set subfile backup for client nodes)
- SET SUMMARYRETENTION (Set number of days to keep data in activity summary table)
- SET TAPEALERTMSG (Set tape alert messages on or off)
- SET TOCLOADRETENTION (Set load retention period for table of contents)
- SET VMATRISKINTERVAL (Specifies the at-risk mode for an individual VM filespace)

SET ACCOUNTING (Set accounting records on or off)

Use this command to determine whether an accounting record is created every time a client node session ends. An accounting record tracks the amount of storage used by a client node session.

Use the QUERY STATUS command to determine whether accounting records are generated. At installation, this value is set to OFF.

The accounting records are stored in an accounting file named dsmaccnt.log.

AIX Linux The environment variable, DSMSERV_ACCOUNTING_DIR, specifies the directory where the accounting file is located.

Windows A registry entry controls the location of the accounting log.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ACCounting--+-ON--+-----------------------------------><
```

```
                    '-OFf-'
```

Parameters

ON
: Specifies that the server creates an accounting record every time a client node session ends.

OFf
: Specifies that the server does not create accounting records.

Example: Create accounting records

To create an accounting record at the end of each client node session issue the command:

```
set accounting on
```

Related commands

Table 1. Commands related to SET ACCOUNTING

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET ACTLOGRETENTION (Set the retention period or the size of the activity log)

Use this command to manage the activity log records by date or size. The activity log contains normal activity messages generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

Activity log information includes messages, such as the following:

- Client session starts and ends
- Migration starts and ends
- Diagnostic error messages
- Scheduled administrative command output

At server installation, activity log management is retention-based, and the retention period is set to 30 days.

You can choose to adjust the length of time that the activity log retains messages to avoid insufficient or outdated data. The server automatically removes the messages from the activity log after the retention period passes.

Alternatively, you can choose to limit the total size of the activity log to control the amount of space occupied by the activity log. The server will periodically remove the oldest activity log records until the activity log size no longer exceeds the configured maximum size allowed.

You can issue the QUERY STATUS command to display the current number of records in the activity log and the size (in megabytes) that the activity log currently occupies.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                                .-Mgmtstyle--=--Date-----.
>>-Set ACTlogretention--number--+------------------------+-----><
                                '-Mgmtstyle--=--+-Date-+-'
                                                '-Size-'
```

Parameters

number (Required)
: Specifies the number of days to retain messages in the activity log when the log is managed by date, or specifies the maximum size of the activity log when it is managed by size. With retention-based management, a value of 1 specifies to retain the activity log records only for the current day. With size-based management, a value of 1 specifies a maximum size of 1 MB for the activity log. You can specify a number from 0 to 9999. A value of 0 disables activity log retention.

Mgmtstyle
: Specifies whether activity log management is retention-based or size-based. This parameter is optional. The default is DATE. Possible values are:

  Date
  : Specifies that activity log management is retention-based.

  Size
  : Specifies that activity log management is size-based.

Example: Set the activity log retention period

Set the server to retain activity log records for 60 days. Issue the command:

```
set actlogretention 60
```

Example: Set the activity log size

Set the server to limit the size of the activity log to 300 MB. Issue the command:

```
set actlogretention 300 mgmtstyle=size
```

Related commands

Table 1. Command related to SET ACTLOGRETENTION

Command	Description
QUERY ACTLOG	Displays messages from the server activity log.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET ALERTACTIVEDURATION (Set the duration of an active alert)

Use this command to specify how long an alert remains active before it is becomes inactive. If an active alert is triggered again, the duration is restarted.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTACtiveduration -number_mins------------------------><
```

Parameters

number_mins (Required)
: Specifies the number of minutes that an alert remains active before it is becomes inactive. Specify a value from 1 to 20160. The initial server default value is 480 minutes.

Set the duration of an active alert to one day

Issue the following command to specify that alerts remain active for 1440 minutes before they change to inactive status:

```
set alertactiveduration 1440
```

Related commands

Table 1. Commands related to SET ALERTACTIVEDURATION

Command	Description
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)	Specifies how long an alert remains inactive before it is closed.
SET ALERTCLOSEDDURATION (Set the duration of a closed alert)	Specifies how long an alert remains closed before it is deleted.
SET ALERTMONITOR (Set the alert monitor to on or off)	Specifies whether alert monitoring is set to on or off.
SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)	Specifies how often the alert monitor updates and prunes alerts from the database.

SET ALERTCLOSEDDURATION (Set the duration of a closed alert)

Use this command to specify how long an alert remains closed before it is deleted.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTCLosedduration -number_mins------------------------><
```

Parameters

number_mins (Required)
: Specifies the number of minutes that an alert remains closed before it is deleted. Setting the value to 0 causes alerts to be deleted immediately after they are closed. Specify a value from 0 to 99999. The default value is set to 60 minutes when the IBM Spectrum Protect™ server database is initially formatted.

Delete alerts two hours after they are closed

Specify that alerts remain closed for 120 minutes before they are deleted:

```
set alertclosedduration 120
```

Related commands

Table 1. Commands related to SET ALERTCLOSEDDURATION

Command	Description
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET ALERTACTIVEDURATION (Set the duration of an active alert)	Specifies how long an alert remains active before it is moved to inactive status.
SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)	Specifies how long an alert remains inactive before it is closed.
SET ALERTMONITOR (Set the alert monitor to on or off)	Specifies whether alert monitoring is set to on or off.

Command	Description
SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)	Specifies how often the alert monitor updates and prunes alerts from the database.

SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)

Use this command to enable alerts to be sent to specified administrators by email.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTEMail--+-ON--+-------------------------------------><
                   '-OFf-'
```

Parameters

ON
: Specifies that alerts can be sent to specified administrators by email.

OFf
: Specifies that alerts cannot be sent to specified administrators by email. When the server database is initially formatted, the ALERTEMAIL setting is set to OFF.

Enable alerts to be sent to the administrator when they occur

Enable alerts to be sent by email by issuing the following command:

```
SET ALERTEMAIL ON
```

Related commands

Table 1. Commands related to SET ALERTEMAIL

Command	Description
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET ALERTEMAILFROMADDR (Set the email address of the sender)	Specifies the email address of the alert sender.
SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)	Specifies the SMTP mail server host name that is used to send alerts by email.
SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)	Specifies the SMTP mail server port that is used to send alerts by email.
SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)	Specifies the administrators that want to receive alert summaries by email.

SET ALERTEMAILFROMADDR (Set the email address of the sender)

Use this command to specify the email address of the alert sender.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTEMAILFRomaddr -email_address----------------------><
```

Parameters

email_address (Required)
: Specifies the email address of the sender. Email addresses are in the form of *name@domain*. Email names, including the address, cannot exceed 64 characters in length, and the domain name cannot exceed 255 characters in length.

Specify the email address of the alert sender

Specify the email address of the sender by issuing the following command:

```
set alertemailfromaddr djadmin@mydomain.com
```

Related commands

Table 1. Commands related to SET ALERTEMAILFROMADDR

Command	Description
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)	Enables alerts to be sent by email to specified administrators.
SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)	Specifies the SMTP mail server host name that is used to send alerts by email.
SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)	Specifies the SMTP mail server port that is used to send alerts by email.
SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)	Specifies the administrators that want to receive alert summaries by email.

SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)

Use this command to specify the Simple Mail Transfer Protocol (SMTP) mail server host name that is used to send the alert email.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTEMAILSMTPHost--host_name---------------------------><
```

Parameters

host_name (Required)
: Specifies the SMTP mail server host name.

Specify the host name for the SMTP mail server as mail.domain.com

Specify `mail.domain.com` as the SMTP mail server, by issuing the following command:

```
set alertemailsmtphost mail.domain.com
```

Related commands

Table 1. Commands related to SET ALERTEMAILSMTPHOST

Command	Description
SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)	Enables alerts to be sent by email to specified administrators.
SET ALERTEMAILFROMADDR (Set the email address of the sender)	Specifies the email address of the alert sender.
SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)	Specifies the SMTP mail server port that is used to send alerts by email.
SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)	Specifies the administrators that want to receive alert summaries by email.

SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)

Use this command to specify the port number for the SMTP mail server. This mail server is used to send the alerts by email.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTEMAILSMTPPort--tcp_port---------------------------><
```

Parameters

tcp_port (Required)
Specifies the port number of the SMTP mail server. Specify a value of 1 through 32767. The default port number is 25.

Specify the port number of the SMTP mail server

Specify port number 450 as your SMTP mail server by issuing the following command:

```
set alertemailsmtpport 450
```

Related commands

Table 1. Commands related to SET ALERTEMAILSMTPPORT

Command	Description
SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)	Enables alerts to be sent by email to specified administrators.
SET ALERTEMAILFROMADDR (Set the email address of the sender)	Specifies the email address of the alert sender.
SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)	Specifies the SMTP mail server host name that is used to send alerts by email.
SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)	Specifies the administrators that want to receive alert summaries by email.

SET ALERTSUMMARYTOADMINS (Set the list of administrators to receive alert summaries by email)

Use this command to specify the administrators that want to receive alert summaries by email, every hour.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTSUMMARYToadmins--+-admin_name-+--------------------><
                             '-,----------'
```

Parameters

admin_name (Required)
: Specifies the administrator name that wants to receive alert summaries by email. You can specify up to three administrator names by separating them with commas and no intervening spaces.

Specify two administrators to receive alert summaries

Specify that administrators HARRY and COLIN want to receive alert summaries, by issuing the following command:

```
set alertsummarytoadmins HARRY,COLIN
```

Related commands

Table 1. Commands related to SET ALERTSUMMARYTOADMINS

Command	Description
SET ALERTEMAIL (Set the alert monitor to email alerts to administrators)	Enables alerts to be sent by email to specified administrators.
SET ALERTEMAILFROMADDR (Set the email address of the sender)	Specifies the email address of the alert sender.
SET ALERTEMAILSMTPHOST (Set the SMTP mail server host name)	Specifies the SMTP mail server host name that is used to send alerts by email.
SET ALERTEMAILSMTPPORT (Set the SMTP mail server host port)	Specifies the SMTP mail server port that is used to send alerts by email.

SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)

Use this command to specify how long an alert remains inactive. After the inactive duration is past, the alert is closed.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTINactiveduration -number_mins----------------------><
```

Parameters

number_mins (Required)
: Specifies the number of minutes that an alert remains inactive before it is closed. You can specify a value in the range 1 - 20160. The initial server default value is 480 minutes.

Change alert status from inactive to closed after 60 minutes

Issue the following command to specify that an alert remains in inactive status for 60 minutes before it changes to closed status:

```
set alertinactiveduration 60
```

Related commands

Table 1. Commands related to SET ALERTINACTIVEDURATION

Command	Description
SET ALERTACTIVEDURATION (Set the duration of an active alert)	Specifies how long an alert remains active before it is moved to inactive status.
SET ALERTCLOSEDDURATION (Set the duration of a closed alert)	Specifies how long an alert remains closed before it is deleted.
SET ALERTMONITOR (Set the alert monitor to on or off)	Specifies whether alert monitoring is set to on or off.
SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)	Specifies how often the alert monitor updates and prunes alerts from the database.

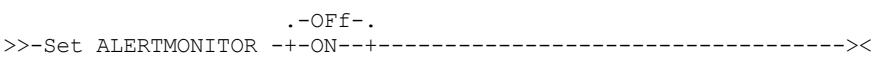
SET ALERTMONITOR (Set the alert monitor to on or off)

Use this command to turn the alert monitor on or off.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

ON
: Specifies that the IBM Spectrum Protect™ server monitors alerts.

OFf
: Specifies that the IBM Spectrum Protect server does not monitor alerts. When the IBM Spectrum Protect server database is initially formatted, the alert monitoring setting is set to OFF.

Turn on alert monitoring

Turn on alert monitoring by issuing the following command:

```
set alertmonitor on
```

Related commands

Table 1. Commands related to SET ALERTMONITOR

Command	Description
SET ALERTACTIVEDURATION (Set the duration of an active alert)	Specifies how long an alert remains inactive before it is closed.
SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)	Specifies how long an alert remains inactive before it is closed.
SET ALERTCLOSEDDURATION (Set the duration of a closed alert)	Specifies how long an alert remains closed before it is deleted.
SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)	Specifies how often the alert monitor updates and prunes alerts from the database.

SET ALERTUPDATEINTERVAL (Set how often the alert monitor updates and prunes alerts)

Use this command to specify how often the alert monitor updates and prunes alerts that are stored in the IBM Spectrum Protect™ server database.

During this check interval, the alert monitor examines each alert on the server and completes the following actions:

- The alert monitor determines whether the active or inactive durations elapsed. If the specified duration elapses, the alert status is updated to the next state. For example:
  - Active to Inactive
  - Inactive to Closed
- If an alert is closed for the duration that is specified by the SET ALERTCLOSEDDURATION command, the alert is deleted.

You can use the QUERY MONITORSETTINGS command to determine whether alert monitoring is on. Use the SET ALERTMONITOR command to turn on alert monitoring.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ALERTUPDateinterval -number_mins------------------------><
```

Parameters

number_mins (Required)
: Specifies the length of time, in minutes, that the monitor waits before alerts are updated and pruned on the server. Specify a value from 1 to 9999. The server has an initial default value of 10 minutes.

Set alert update interval to 60 minutes

Specify that alerts are updated every hour by issuing the following command:

```
set alertupdateinterval  60
```

Related commands

Table 1. Commands related to SET ALERTUPDATEINTERVAL

Command	Description
SET ALERTACTIVEDURATION (Set the duration of an active alert)	Specifies how long an alert remains active before it is moved to inactive status.
SET ALERTINACTIVEDURATION (Set the duration of an inactive alert)	Specifies how long an alert remains inactive before it is closed.
SET ALERTCLOSEDDURATION (Set the duration of a closed alert)	Specifies how long an alert remains closed before it is deleted.
SET ALERTMONITOR (Set the alert monitor to on or off)	Specifies whether alert monitoring is set to on or off.

SET ARCHIVERETENTIONPROTECTION (Activate data retention protection)

Use this command to activate and deactivate archive data retention protection. The server cannot contain any data in order for this command to work. At installation, the value is set to OFF.

When archive data retention protection is active:

- Only archive copies can be stored on the server.
- No archive copy can be deleted until the RETVER parameter in the DEFINE COPYGROUP (archive) command is satisfied.

Defining storage pools of type RECLAMATIONTYPE=SNAPLOCK is only supported on servers with data retention protection enabled.

Use the QUERY STATUS command to display the status of archive data retention protection.

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-Set ARCHIVERETENTIONPROTECTion -+-OFf-+---------------------><
                                   '-ON--'
```

Parameters

OFf
: Specifies that archive data retention protection is not active.

ON
: Specifies the archive data retention protection is active.

Example: Activate data retention protection

Activate archive data retention protection by issuing the following command:

```
set archiveretentionprotection on
```

Related commands

Table 1. Commands related to SET ARCHIVERETENTIONPROTECTION

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
AUDIT VOLUME	Compares database and storage pool information, and optionally, resolves any inconsistencies.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

SET ARREPLRULEDEFAULT (Set the server replication rule for archive data)

Use this command to set the server replication rule for archive data.

Restriction: The replication rule that you set with this command is applied only if file space rules and client node rules for archive data are set to DEFAULT.

Issue this command on the server that acts as a source for replicated data.

You can specify a normal-priority replication rule or a high-priority replication rule. In a replication process that includes both normal-priority and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

For example, suppose that your client nodes contain archive data and backup data. Replication of the archive data is a higher priority than the backup data. To prioritize the archive data, issue the SET ARREPLRULEDEFAULT command and specify the ALL_DATA_HIGH_PRIORITY replication rule. To prioritize the backup data, issue the SET BKREPLRULEDEFAULT command and specify the ALL_DATA replication rule for backup data. The ALL_DATA rule for backup data replicates backup data with a normal priority.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set ARREPLRuledefault--+-ALL_DATA----------------+----------><
                          +-ALL_DATA_HIGH_PRIORITY-+
                          '-NONE--------------------'
```

Parameters

ALL_DATA
: Replicates archive data with a normal priority.

ALL_DATA_HIGH_PRIORITY
: Replicates archive data with a high priority.

NONE
: Archive data is not replicated.

Example: Set the server replication rule for archive data

Set up the default rule for archive data to replicate with a high priority.

```
set arreplruledefault all_data_high_priority
```

Related commands

Table 1. Commands related to SET ARREPLRULEDEFAULT

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLRULE	Displays information about node replication rules.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET BKREPLRULEDEFAULT	Specifies the server node-replication rule for backup data.
SET SPREPLRULEDEFAULT	Specifies the server node-replication rule for space-managed data.

Command	Description
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE REPLRULE	Enables or disables replication rules.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

SET BKREPLRULEDEFAULT (Set the server replication rule for backup data)

Use this command to set the server replication rule for backup data.

Restriction: The replication rule that you set with this command is applied only if file space rules and client node rules for backup data are set to DEFAULT.

Issue this command on the server that acts as a source for replicated data.

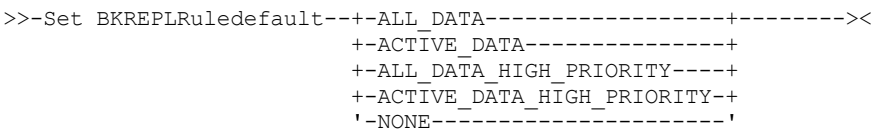
You can specify normal-priority replication rules or high-priority replication rules. In a replication process that includes both normal and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

For example, suppose that your client nodes contain archive data and active backup data. Replication of the active backup data is a higher priority than the archive data. To prioritize the backup data, issue the SET BKREPLRULEDEFAULT command and specify the ACTIVE_DATA_HIGH_PRIORITY replication rule. To prioritize the archive data, issue the SET ARREPLRULEDEFAULT command and specify the ALL_DATA replication rule for archive data. The ALL_DATA rule for archive data replicates archive data with a normal priority.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

ALL_DATA
: Replicates active and inactive backup data. The data is replicated with normal priority.

ACTIVE_DATA
: Replicates active backup data. The data is replicated with normal priority.
Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

- When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
- When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
- When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
: Replicates active and inactive backup data. Data is replicated with a high priority.

ACTIVE_DATA_HIGH_PRIORITY

This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

NONE
: Backup data is not replicated.

Example: Set the server replication rule for backup data

Set up the default rule for backup data to replicate only active data and to replicate the data with a high priority.

```
set bkreplruledefault active_data_high_priority
```

Related commands

Table 1. Commands related to SET BKREPLRULEDEFAULT

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLRULE	Displays information about node replication rules.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET ARREPLRULEDEFAULT	Specifies the server node-replication rule for archive data.
SET REPLRETENTION	Specifies the retention period for replication history records.
SET SPREPLRULEDEFAULT	Specifies the server node-replication rule for space-managed data.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE REPLRULE	Enables or disables replication rules.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

SET CLIENTACTDURATION (Set the duration period for the client action)

Use this command to specify the duration for the schedule that was defined with the DEFINE CLIENTACTION command. A client action defines a schedule that runs one time on a client.

The program deletes these event records whether or not the client has processed the schedule. However, the schedules are not deleted until after the first event records are deleted. The retention period for events defaults to 10 days at installation.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET CLIENTACTDuration--days---------------------------------><
```

Parameters

days (Required)
: Specifies the number of days during which the schedule for the client action is active. You can specify an integer from 0 to 999. The default is 5 days.

The number of days you specify determines how long the database retains the schedule before deletion. A value of 0 indicates that the schedule duration is indefinite, and the schedule and associations are not deleted from the database.

Example: Set a 15–day duration period for the client action

To specify that the schedule for the client action be active for 15 days issue the following command.

```
set clientactduration 15
```

Related commands

Table 1. Commands related to SET CLIENTACTDURATION

Command	Description
DEFINE CLIENTACTION	Defines a command to be performed at a client node.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET CONFIGMANAGER (Specify a configuration manager)

Use this command to specify whether a server is a configuration manager. On a configuration manager, you can define configuration profiles to which other servers can subscribe.

You cannot designate a server as a configuration manager if the server subscribes to one or more profiles on another configuration manager.

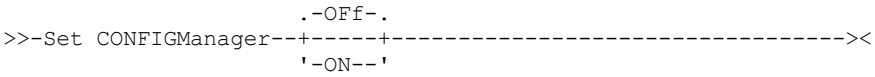
If a server is a configuration manager, you cannot change this designation until you delete all profiles, including the default profile.

Issue the QUERY STATUS command to determine if a server is a configuration manager. When a server is installed, it is not designated as a configuration manager.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

ON
: Specifies that the server is a configuration manager.

  When you designate a server as a configuration manager, IBM Spectrum Protect™ creates a default profile named DEFAULT_PROFILE and associates with the profile all servers and server groups defined on the configuration manager. You can modify or delete the default profile.

OFf
: Specifies that the server is not a configuration manager.

Example: Specify a configuration manager

Designate a server as a configuration manager.

```
set configmanager on
```

Related commands

Table 1. Commands related to SET CONFIGMANAGER

Command	Description
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET CONFIGREFRESH	Specifies a time interval for managed servers to contact configuration managers.

SET CONFIGREFRESH (Set managed server configuration refresh)

Use this command on a managed server to specify how often that server contacts its configuration manager for updated configuration information.

To display the current setting, issue the QUERY STATUS command. At installation, the interval is set to 60 minutes.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set CONFIGRefresh--minutes---------------------------------><
```

Parameters

minutes (Required)
Specifies the interval, in minutes, before a managed server contacts its configuration manager for configuration updates. Specify an integer from 0 to 10000.

- If the value is greater than 0, the managed server immediately contacts the configuration manager. The next contact occurs when the specified interval is reached.
- If the value is 0, the managed server does not contact the configuration manager.

This value is ignored if the server does not subscribe to at least one profile on a configuration manager.

Example: Set a 45–minute refresh interval

Specify that a managed server contacts its configuration manager every 45 minutes.

```
set configrefresh 45
```

Related commands

Table 1. Commands related to SET CONFIGREFRESH

Command	Description
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
NOTIFY SUBSCRIBERS	Notifies servers to refresh their configuration information.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UPDATE PROFILE	Changes the description of a profile.

SET CONTEXTMESSAGING (Set message context reporting on or off)

Use this command to get additional information when ANR9999D messages occur. IBM Spectrum Protect™ polls the server components for information that includes process name, thread name, session ID, transaction data, locks that are held, and database tables that are in use.

Note: When consecutive messages are issued from the same code area by the same thread, only the first of these messages will report the context information.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set CONTEXTmessaging--+-ON--+------------------------------><
                         '-OFf-'
```

Parameters

ON
: Specifies to enable message context reporting.

OFf
: Specifies to disable message context reporting.

Example: Set message context reporting on or off

Turn on context messaging to receive additional information that could help determine the cause of ANR9999D messages.

```
set contextmessaging on
```

Related commands

Table 1. Commands related to SET CONTEXTMESSAGING

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET CPUINFOREFRESH (Refresh interval for the client workstation information scan)

Use this command to specify the number of days between client scans of workstation information that is used to estimate the processor value unit (PVU).

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set CPUINFOREFRESH--days-----------------------------------><
```

Parameters

days (Required)

Specifies the number of days between scans for client devices. To retrieve the current setting, issue the QUERY STATUS command. The possible values are 1 - 9999. The default is 180.

Example: Set the amount of time before the next refresh to 90 days

```
SET CPUINFOREFRESH 90
```

Related commands

Table 1. Commands related to SET CPUINFOREFRESH

Command	Description
QUERY PVUESTIMATE	Displays an estimate of the client-devices and server-devices being managed.

SET CROSSDEFINE (Specifies whether to cross-define servers)

Use this command to specify whether a server is automatically defined to another server.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set CROSSDefine--+-ON--+-----------------------------------><
                    '-OFf-'
```

Parameters

ON
: Specifies that a server may be cross-defined to another server. To automatically define one server to another, you must also permit cross defining in the server definition.

OFf
: Specifies that a server may not be cross-defined to another server.

Example: Specifies whether to cross-define servers

Set cross define on to allow a server to be cross-defined to another server.

```
set crossdefine on
```

Related commands

Table 1. Command related to SET CROSSDEFINE

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.
SET SERVERHLADDRESS	Specifies the high-level address of a server.
SET SERVERLLADDRESS	Specifies the low-level address of a server.
SET SERVERPASSWORD	Specifies the server password.

SET DBRECOVERY (Set the device class for automatic backups)

Use this command to specify the device class and number of data streams to be used for automatic database backups. You can also use this command to configure the BACKUP DB command to automatically back up the master encryption key for the server.

The master encryption key is used to encrypt data in directory-container and cloud-container storage pools, and to encrypt sensitive information in the server database. If you do not back up the master encryption key, you might not be able to access any of these encrypted items if a disaster occurs.

If you run the BACKUP DB command, and the device class is not the one that is specified in the SET DBRECOVERY command, a warning message is returned. However, the backup operation continues and is not affected.

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

```
>>-SET DBRECOVery--device_class_name---------------------------->

   .-NUMStreams--=--1------.  .-COMPress--=--No------.
>--+----------------------+--+---------------------+---------->
   '-NUMStreams--=--number-'  '-COMPress--=--+-No--+-'
                                             '-Yes-'

   .-PROTECTKeys--=--Yes-----.
>--+-------------------------+-------------------------------->
   '-PROTECTKeys--=--+-No--+-'
                     '-Yes-'

>--+---------------------------+------------------------------><
   '-PASSword--=--password_name-'
```

Parameters

device_class_name **(Required)**
: Specifies the device class to use for database backups.

NUMStreams
: Specifies the number of parallel data movement streams to use when you back up the database. The default value is 1, and the maximum number is 32. Increasing this value causes a corresponding increase in the number of database backup sessions to be used and in the number of drives to be used for the device class. A NUMSTREAMS value that is specified in the BACKUP DB command overrides any value set in the SET DBRECOVERY command. The NUMSTREAMS value is used for all types of database backups.
  If a value is specified that is greater than the number of drives available for the device class, the number of available drives are used. The available drives are defined to the device class by the MOUNTLIMIT parameter or by the number of online drives for the specified device class. The session is displayed in the QUERY SESSION output.
  If you increase the number of streams, more volumes are used from the corresponding device class for this operation. Using more volumes might improve the speed of the database backups, but at the cost of more volumes that are not fully used.

COMPress
: Specifies whether volumes are compressed during database backup processing. This parameter is optional. The default value is No. You can specify one of the following values:

  No
  : Specifies that the volumes that are created by the BACKUP DB command are not compressed.

  Yes
  : Specifies that the volumes that are created by the BACKUP DB command are compressed.

  If you specify the COMPRESS parameter on the BACKUP DB command, it overrides any value that is set in the SET DBRECOVERY command. Otherwise, the value that is set in the SET DBRECOVERY command is used.
  Restrictions:

  - Use caution when you specify the COMPRESS parameter. Using compression during database backups can reduce the size of the backup files. However, compression can increase the time to complete database backup processing.
  - Do not back up compressed data to tape. If your system environment stores database backups on tape, set the COMPRESS parameter to No in the SET DBRECOVERY and BACKUP DB commands.

PROTECTKeys

Specifies that database backups include a copy of the master encryption key for the server that is used to encrypt node passwords, administrator passwords, and storage pool data. The master encryption key is stored in the dsmkeydb files. If you lose the dsmkeydb files, nodes and administrators are unable to authenticate with the server because the server is unable to read the passwords that are encrypted by using the master encryption key. In addition, any data that is stored in an encrypted storage pool cannot be retrieved without the master encryption key. This parameter is optional. The default value is Yes. You can specify one of the following values:

No
: Specifies that database backups do not include a copy of the master encryption key for the server.
Attention: If you specify PROTECTKEYS=NO, you must manually back up the master encryption key for the server and make the key available when you implement disaster recovery. You cannot recover from a disaster without the master encryption key.

Yes
: Specifies that database backups include a copy of the master encryption key for the server.
Attention: If you specify PROTECTKEYS=YES, you must also specify the PASSWORD parameter.

PASSword
: Specifies the password that is used to protect the database backups. By default, database backup operations are protected by using a password. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.
Important: Ensure that you remember this password. If you specify a password for database backup, you must specify the same password on the RESTORE DB command to restore the database.

Example: Specify a device class for database backups

Specify the DBBACK device class for database backups. Run the following command:

```
set dbrecovery dbback
```

Example: Specify a device class and number of streams for database backups

Specify the DBBACK device class for database backups, and specify that the backup is to use two data movement streams. Run the following command:

```
set dbrecovery dbback numstreams=2
```

AIX | Linux | Windows

Example: Protect storage pool encryption keys in database backups

Encrypt storage pool data by specifying that database backups include a copy of the master encryption key for the server. Run the following command:

```
set dbrecovery dbback protectkeys=yes password=password_name
```

Related commands

Table 1. Commands related to SET DBRECOVERY

Command	Description
BACKUP DB	Backs up the IBM Spectrum Protect database to sequential access volumes.
QUERY DB	Displays allocation information about the database.
QUERY DBSPACE	Displays information about the storage space defined for the database.

SET DEDUPVERIFICATIONLEVEL (Set the percentage of extents to verify)

Use this command to verify extents sent to the server during client-side data deduplication.

A rogue application that resides on a client system and that imitates the client, API, or GUI application can initiate an attack on the server. To reduce server vulnerability to such attacks, you can specify a percentage of client extents for the server to verify.

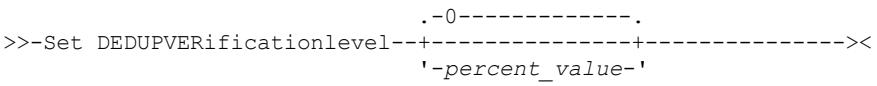
If the server detects that a security attack is in progress, the current session is canceled. In addition, the setting of the DEDUPLICATION parameter on the REGISTER NODE command is changed. The setting is changed from CLIENTORSERVER to SERVERONLY. The SERVERONLY setting disables client-side data deduplication for that node.

The server also issues a message that a potential security attack was detected and that client-side data deduplication was disabled for the node. If client-side data deduplication is disabled, all other client operations (for example, backup operations) continue. Only client-side data deduplication is disabled. If client-side data deduplication is disabled for a node because a potential attack was detected, the server deduplicates the data that is eligible for client-side data deduplication.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

percent_value (Required)
Specify an integer value 0 - 100 to indicate the percentage of client extents to be verified. A value of 0 indicates that no client extents are verified. The default for this command is 0.
Tips:

- Verifying extents consumes processing power and adversely affects server performance. For optimal performance, do not specify values greater than 10 for this command.
- To display the current value for SET DEDUPVERIFICATIONLEVEL, issue the QUERY STATUS command.

Example: Specify a minimum level of data deduplication verification

To specify that 1% of extents created during client-side data deduplication are verified, issue the following command:

```
set dedupverificationlevel 1
```

Example: Turn off data deduplication verification

To specify that none of the extents created during client-side data deduplication are verified, issue the following command:

```
set dedupverificationlevel 0
```

Related commands

Table 1. Commands related to SET DEDUPVERIFICATIONLEVEL

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
QUERY CONTENT	Displays information about files in a storage pool volume.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER NODE	Defines a client node to the server and sets options for that user.
UPDATE NODE	Changes the attributes that are associated with a client node.
UPDATE STGPOOL	Changes the attributes of a storage pool.

SET DEFAULTAUTHENTICATION (Set the default authentication method for REGISTER NODE and REGISTER ADMIN commands)

Use this command to set the default password authentication method for nodes and administrators that are the result of REGISTER NODE or REGISTER ADMIN commands.

If you specify LDAP, you establish the default value for authenticating to an external directory for any new REGISTER NODE or REGISTER ADMIN commands. This command makes it easier to register nodes or administrators when you use an LDAP directory server.
Tip: The default authentication setting can be overwritten when the authentication method is specified in a REGISTER NODE or REGISTER ADMIN command.

Privilege class

To issue this command you must have system privilege.

Syntax

```
>>-SET DEFAULTAUTHentication--+-LOcal-+------------------------><
                              '-LDap--'
```

Parameters

LOcal
: Specifies that any future REGISTER NODE or REGISTER ADMIN commands that you issue use LOCAL as the default authentication parameter value. Locally-authenticated passwords are those stored on the IBM Spectrum Protect™ server. The passwords authenticated locally are not case sensitive.

LDap
: Specifies that any future REGISTER NODE or REGISTER ADMIN commands that you issue use LDAP as the default authentication parameter value. LDAP-authenticated passwords are those stored on an LDAP directory server and are case sensitive.

Example: Set the default password authentication value to LDAP

Specify that any REGISTER NODE or REGISTER ADMIN commands that you issue authenticate passwords with an LDAP directory server.

```
set defaultauthentication ldap
```

Related commands

Table 1. Commands related to SET DEFAULTAUTHENTICATION

Command	Description
SET LDAPPASSWORD	Sets the password for the LDAPUSER.
SET LDAPUSER	Sets the user who oversees the passwords and administrators on the LDAP directory server.
SET LDAPUSER	Sets the user who oversees the passwords and administrators on the LDAP directory server.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
REGISTER NODE	Defines a client node to the server and sets options for that user.

SET DEPLOYPKGMGR (Enable the deployment package manager)

Use this command to enable or disable the deployment package manager. This component downloads client deployment packages from the FTP site for automatic installation by using the Operations Center.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                    .-ON--.
>>-SET DEPLOYPKGMgr--+-OFf-+-----------------------------------><
```

Parameters

ON
: Specifies that the deployment package manager queries the FTP site for new deployment packages and downloads new packages as they become available. This is the default.

OFf
: Specifies that the deployment package manager does not query the FTP site or download new packages. If you disable the deployment package manager while packages are downloading, the active download processes continue to run until they are completed.

Example: Disable the deployment package manager

Disable the deployment package manager by issuing the following command:

```
set deploypkgmgr off
```

Related commands

Table 1. Commands related to SET DEPLOYPKGMGR

Command	Description
QUERY MONITORSETTINGS	Displays information about monitoring alerts and server status settings.
SET DEPLOYREPOSITORY	Specifies the location where client deployment packages are downloaded.

SET DEPLOYREPOSITORY (Set the download path for client deployment packages)

Use this command to specify the location where the automated deployment process downloads the latest client deployment packages. The deployment packages are used to install updates on client systems.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET DEPLOYREPository--path_name-----------------------------><
```

Parameters

path_name (Required)

Specifies the fully qualified path name where deployment packages are downloaded. This path also specifies the location where the server places the files that represent the storage volumes for the client deployment device class. You must specify a path name. If you do not, the server does not download the deployment packages.

When you modify the location where update packages are stored, previously downloaded packages are deleted automatically. Server volumes are deleted as data is pruned or expired.
Important: Do not manually delete files with a file name extension of .BFS. BFS files are volumes that are managed by the server, and they contain archive data that is expired or pruned automatically.

Example: Specify a path name

Specify `/source/packages/` as the location where deployment packages are downloaded. The same location is used for the IBM_DEPLOY_CLIENT_IMPORT device class, which is used for client deployment.

```
set deployrepository /source/packages/
```

Related commands

Table 1. Commands related to SET DEPLOYREPOSITORY

Command	Description
QUERY MONITORSETTINGS	Displays information about monitoring alerts and server status settings.
SET DEPLOYMAXPKGS	Specifies the maximum number of client deployment packages that are downloaded and stored on the server.

SET DEPLOYMAXPKGS (Set the maximum number of client deployment packages to store)

Use this command to specify the maximum number of client installable deployment packages that are downloaded and stored on the server.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET DEPLOYMAXPkgs--number-----------------------------------><
```

Parameters

number

Specifies the maximum number of deployment packages that are stored in the deployment repository for each product version. The minimum number of packages is 1, and the maximum number is 4. If you decrease the number, older versions of the packages are removed the next time packages are refreshed. It can take up to one day for packages to refresh. The default number is 4.

Example: Specify the maximum number of deployment packages

Specify 3 as the maximum number of deployment packages that are downloaded and stored.

```
set deploymaxpkgs 3
```

Related commands

Table 1. Commands related to SET DEPLOYMAXPKGS

Command	Description
QUERY MONITORSETTINGS	Displays information about monitoring alerts and server status settings.
SET DEPLOYREPOSITORY (Set the download path for client deployment packages)	Specifies the location where client deployment packages are downloaded.

SET DISSIMILARPOLICIES (Enable the policies on the target replication server to manage replicated data)

Use the SET DISSIMILARPOLICIES command to enable the policies that are defined on the target replication server to manage replicated client-node data. If you do not use the policies on the target replication server, replicated client-node data is managed by policies on the source replication server.

Ensure that IBM Spectrum Protect™, Version 7.1.1 or later, is installed on the source and target replication servers before you issue this command. Issue this command on the source replication server.

Before you use the policies that are defined on a target replication server, you must issue the VALIDATE REPLPOLICY command for that target replication server. This command displays the differences between the policies for the client nodes on the source replication server and policies on the target replication server. You can modify the policies on the target replication server before you enable these policies to manage replicated client-node data.

To obtain the name of the target replication server for which you want to manage data and to check whether the policies on the target replication server are set to ON, use the QUERY REPLSERVER command. At installation, the value is set to OFF.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                                                .-OFf-.
>>-Set DISSIMILARPolicies--target_server_name--+-----+---------><
                                                +-OFf-+
                                                '-ON--'
```

Parameters

target_server_name (Required)
: Specifies the name of the target replication server for which you want to enable the policies.

ON
: Specifies that replicated client-node data is managed by the policies that are defined on the target replication server.

OFf
: Specifies that replicated client-node data is managed by the policies that are defined on the source replication server. Off is the default value.

Example: Use the policies on a target replication server

To managed replicated client-node data from the target replication server, CVTCVS_LXS_SRV2, issue the following command on the source replication server:

```
set dissimilarpolicies CVTCVS_LXS_SRV2 on
```

Related commands

Table 1. Commands related to SET DISSIMILARPOLICIES

Command	Description
QUERY REPLSERVER	Displays information about replicating servers.

Command	Description
VALIDATE REPLPOLICY	Verifies the policies on the target replication server.

SET DRMACTIVEDATASTGPOOL (Specify the active-data pools to be managed by DRM)

Use this command to specify names of the active-data pools to be recovered after a disaster. IBM Spectrum Protect™ uses these names if the PREPARE , MOVE DRMEDIA, or QUERY DRMEDIA command does not include the ACTIVEDATASTGPOOL parameter.

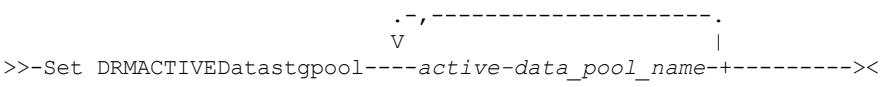
By default, volumes in active-data pools are not eligible for processing by disaster recovery manager. To process active-data pool volumes, you must issue the SET DRMACTIVEDATASTGPOOL command, or you must use the ACTIVEDATASTGPOOL command-line parameter on the MOVE DRMEDIA, QUERY DRMEDIA, or PREPARE command.

Use the QUERY DRMSTATUS command to display the current settings.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

active-data_pool_name (Required)
: Specifies the active-data pool names. Separate multiple names with commas with no intervening spaces. You can use wildcard characters. The specified names will overwrite any previous settings. If you enter a null string (""), all current names are removed, and no active-data pool volumes in MOUNTABLE state are processed if they were not explicitly entered as MOVE DRMEDIA , QUERY DRMEDIA, or PREPARE command parameters.

Example: Set an eligible active-data pool

Set ACTIVEDATAPOOL1 as the eligible active-data pool.

```
set drmactivedatapool activedatastgpool1
```

Related commands

Table 1. Commands related to SET DRMACTIVEDATASTGPOOL

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
PREPARE	Creates a recovery plan file.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.
SET DRMPRIMSTGPOOL	Specifies that primary storage pools are managed by DRM.

SET DRMCHECKLABEL (Specify label checking)

Use this command to specify whether IBM Spectrum Protect™ reads the labels of sequential media checked out by the MOVE DRMEDIA command. At installation, the value of the DRMCHECKLABEL is set to YES.

Use the QUERY DRMSTATUS command to check the current setting.

AIX Linux This command does not apply to 349X device types.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                        .-Yes-.
>>-Set DRMCHECKLabel--+-----+---------------------------------><
                      +-Yes-+
                      '-No--'
```

Parameters

Yes
: Specifies that IBM Spectrum Protect reads the labels of sequential media checked out by the MOVE DRMEDIA command.

No
: Specifies that IBM Spectrum Protect does not read the labels of sequential media checked out by the MOVE DRMEDIA command.

Example: Specify no label checking

Specify that no label checking is completed.

```
set drmchecklabel no
```

Related commands

Table 1. Commands related to SET DRMCHECKLABEL

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMCMDFILENAME (Specify the name of a file to contain commands)

Use this command to name a file that can contain the commands created when the MOVE DRMEDIA or QUERY DRMEDIA commands are issued. If the SET DRMCMDFILENAME is not issued, the MOVE DRMEDIA or QUERY DRMEDIA command generates a file name.

Use the QUERY DRMSTATUS command to display the current command file name.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMCMDFilename--file_name-------------------------------><
```

Parameters

file_name (Required)

AIX Linux Specifies a full path name for a file to contain the commands created by the MOVE DRMEDIA or QUERY DRMEDIA command.

Windows Specifies a full path name for a file to contain the commands created by the MOVE DRMEDIA or QUERY DRMEDIA command. The file name can be up to 259 characters.

Attention: If a file of the same name already exists, MOVE DRMEDIA or QUERY DRMEDIA command tries to use it, and the existing data is overwritten.

Example: Specify a file name to contain DRMEDIA commands

AIX Linux Specify a file name of /adsm/drm/orm/exec.cmds.

```
set drmcmdfilename /adsm/drm/orm/exec.cmds
```

Windows Specify a file name of c:\drm\orm\exec.cmd.

```
set drmcmdfilename c:\drm\orm\exec.cmd
```

Related commands

Table 1. Commands related to SET DRMCMDFILENAME

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

AIX Linux Windows

SET DRMCOPYCONTAINERSTGPOOL (Specify the container-copy storage pools to be processed by DRM commands)

Use this command to specify the container-copy storage pools to be processed by the MOVE DRMEDIA or QUERY DRMEDIA command when that command does not include the COPYCONTAINERSTGPOOL parameter.

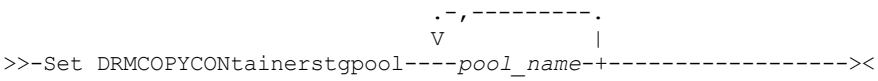
By default, volumes in container-copy storage pools are not processed by the MOVE DRMEDIA and QUERY DRMEDIA commands. To process the volumes, you must issue the SET DRMCOPYCONTAINERSTGPOOL command, or you must use the COPYCONTAINERSTGPOOL parameter on the MOVE DRMEDIA or QUERY DRMEDIA command.

Tip: To display the current settings, use the QUERY DRMSTATUS command.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

pool_name (Required)
: Specifies the names of the container-copy storage pools. Separate multiple names with commas and no intervening spaces. You can use wildcard characters. The specified names replace any previous setting. If you enter a null string (""), all current names are removed.

Example: Specify storage pools to be processed by the MOVE DRMEDIA and QUERY DRMEDIA commands

Set CONTCOPY1 and CONTCOPY2 as the container-copy storage pools to be processed.

```
set drmcopycontainerstgpool contcopy1,contcopy2
```

Related commands

Table 1. Commands related to SET DRMCOPYCONTAINERSTGPOOL

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMCOPYSTGPOOL (Specify the copy storage pools to be managed by DRM)

Use this command to specify names of the copy storage pools to be recovered after a disaster. IBM Spectrum Protect™ uses these names if the PREPARE command does not include the COPYSTGPOOL parameter.

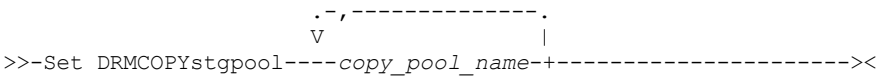
If the MOVE DRMEDIA or QUERY DRMEDIA command does not include the COPYSTGPOOL parameter, the command processes the volumes in the MOUNTABLE state that are in the copy storage pool named by the SET DRMCOPYSTGPOOL command. At installation, all copy storage pools are eligible for DRM processing.

Use the QUERY DRMSTATUS command to display the current settings.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

copy_pool_name (Required)
: Specifies the copy storage pool names. Separate multiple names with commas and no intervening spaces. You can use wildcard characters. The specified names replace any previous setting. If you enter a null string (""), all current names are removed, and all copy storage pools are eligible for processing.

Example: Set an eligible copy storage pool

Set COPYSTGPOOL1 as the eligible copy storage pool.

```
set drmcopystgpool copystgpool1
```

Related commands

Table 1. Commands related to SET DRMCOPYSTGPOOL

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.
SET DRMPRIMSTGPOOL	Specifies that primary storage pools are managed by DRM.

SET DRMCOURIERNAME (Specify the courier name)

Use this command to specify the courier name. At installation, this name is set to COURIER. The MOVE DRMEDIA command uses the courier name to set the location of volumes that are moving to the COURIER state.

You can use the QUERY DRMSTATUS to see the name of the courier.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMCOUriername--courier_name----------------------------><
```

Parameters

courier_name (Required)
: Specifies the name of the courier. The name can be up to 255 characters. Enclose the name in quotation marks if it contains any blank characters.

Example: Set the courier name

Set the name of the courier to Joe's Courier Service.

```
set drmcouriername "Joe's Courier Service"
```

Related commands

Table 1. Commands related to SET DRMCOURIERNAME

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)

Use this command to specify when a database backup series is eligible to be expired.

The value set by this command applies to both a snapshot and a full plus incremental database backup series. Any type of database backup series is eligible for expiration if all of the following are true:

- The age of the last volume of the series exceeds the expiration value set with the SET DRMDBBACKUPEXPIREDAYS command and the value that is specified for the DELgraceperiod parameter in the DEFINE SERVER command. The DELgraceperiod parameter applies only to remote database backups. The default value for the DELgraceperiod parameter is 5 days. For example, if you set the value for the SET DRMDBBACKUPEXPIREDAYS command to 7 days and set the value for the DELgraceperiod parameter to 6 days, the remote database backup series does not expire until 13 days elapse.
- For volumes that are not virtual volumes, all volumes in the series are in the VAULT state.
- The volume is not part of the most recent database backup series.

Remember: The most recent backup series of either type is not deleted.
See the MOVE DRMEDIA command for more information on the expiration of database backup volumes that are not virtual volumes. See the EXPIRE INVENTORY command for more information on expiration of database backup volumes that are virtual volumes.

Use the QUERY DRMSTATUS to see the number of days specified.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMDBBackupexpiredays--days-----------------------------><
```

Parameters

days (Required)
Specifies the number of days that must elapse since a database series was created before it is eligible to be expired. The number of days must match the volume reuse delay period for copy storage pools that are managed by disaster recovery manager. Specify an integer value 0 - 9999.

Example: Set the database backup series expiration

Set the database backup series expiration value to 60.

```
set drmdbbackupexpiredays 60
```

Related commands

Table 1. Commands related to SET DRMDBBACKUPEXPIREDAYS

Command	Description
DSMSERV RESTORE DB	Restores an IBM Spectrum ProtectIBM Spectrum Protect™ database.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
DEFINE SERVER	Defines a server for server-to-server communications.

SET DRMFILEPROCESS (Specify file processing)

Use this command to specify if the MOVE DRMEDIA or QUERY DRMEDIA command should process database backup volumes and copy storage pool volumes that are associated with a FILE device class. At installation, the value is set to NO. Use the QUERY DRMSTATUS to determine the current setting.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                        .-No--.
>>-Set DRMFILEProcess--+-----+--------------------------------><
```

```
          +-No--+
          '-Yes-'
```

Parameters

No
: Specifies that the MOVE DRMEDIA and QUERY DRMEDIA commands does not process database backup and copy storage pool volumes that are associated with a FILE device class. This is the default.

Yes
: Specifies that the MOVE DRMEDIA and QUERY DRMEDIA commands process database backup and copy storage pool volumes that are associated with a FILE device class.

Example: Specify that the DRMEDIA commands do not include FILE type device classes

Set the file processing value to no.

```
set drmfileprocess no
```

Related commands

Table 1. Commands related to SET DRMFILEPROCESS

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMINSTRPREFIX (Specify the prefix for recovery instructions file names)

Use this command to specify a prefix to the recovery instructions file name. If you issue this command, IBM Spectrum Protect™ uses the specified prefix if the PREPARE command is issued without the INSTRPREFIX parameter.

Use the QUERY DRMSTATUS command to display the current value for the prefix.

AIX Linux the prefix is the current IBM Spectrum Protect server working directory.

Windows If no prefix is set, the prefix is set to the directory representing this instance of the server, which is typically the directory that the server was originally installed from.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMINSTRPrefix--prefix-----------------------------------><
```

Parameters

AIX Linux prefix (Required)

AIX Linux

Specifies a path name prefix for the files that contain the recovery instructions. When processing the PREPARE command, IBM Spectrum Protect appends the name of the appropriate recovery plan file stanza to find the file. The maximum length is 250 characters.

The prefix can be one of the following:

- **Directory path:** End the prefix with a foward slash (/). For example:

  ```
  /adsmsrv/recinstr/
  ```

  For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would be:

  ```
  /adsmsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **Directory path followed by a string:** IBM Spectrum Protect treats the string as part of the file name. For example:

  ```
  /adsmsrv/recinstr/accounts
  ```

  For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would be:

  ```
  /adsmsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **String only:** IBM Spectrum Protect specifies the directory path and appends the appropriate recovery plan file stanza name.
  - IBM Spectrum Protect uses the name of the current working directory. For example, the current working directory is/opt/tivoli/tsm/server/bin. You specify the following:

    ```
    shipping
    ```

    For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would look like this:

    ```
    /opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
    ```

Windows prefix (Required)

Windows

Specifies a path name prefix for the files that contain the recovery instructions. When processing the PREPARE command, IBM Spectrum Protect appends the name of the appropriate recovery plan file stanza to find the file. The maximum length is 200 characters.

The prefix can be one of the following:

- **Directory path:** End the prefix with a back slash (\). For example:

  ```
  c:\adsmsrv\recinstr\
  ```

  For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would be:

  ```
  c:\adsmsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **Directory path followed by a string:** IBM Spectrum Protect treats the string as part of the file name. For example:

  ```
  c:\adsmsrv\recinstr\accounts
  ```

  For the RECOVERY.INSTRUCTIONS.GENERAL file, the resulting file name would be:

  ```
  c:\adsmsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **String only:** IBM Spectrum Protect specifies the directory path and appends the appropriate recovery plan file stanza name. The directory path is the directory representing this instance of the IBM Spectrum Protect server (typically the original IBM Spectrum Protect server installation directory). For example, the directory representing this instance of the server is c:\Program Files\Tivoli\TSM;\server2, and you specify the following prefix:

  ```
  shipping
  ```

  The resulting recovery plan file name is:

  ```
  c:\Program Files\Tivoli\TSM;\server2\shipping.19971115.051421
  ```

Example: Specify the recovery plan prefix

AIX Linux Specify reading the recovery plan instructions from directory /drmplan/primesrv.

```
set drminstrprefix /drmplan/primesrv/
```

Windows Specify reading the recovery plan instructions from directory c:\win32app\ibm\adsm\server2\.

```
set drminstrprefix c:\win32app\ibm\adsm\server2\
```

Related commands

Table 1. Commands related to SET DRMINSTRPREFIX

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMNOTMOUNTABLENAME (Specify the not mountable location name)

Use this command to specify the name of the onsite location for storing the media. At installation, the name is set to NOTMOUNTABLE. Use the QUERY DRMSTATUS command to see the location name.

The location name is used by the MOVE DRMEDIA command to set the location of volumes that are moving to the NOTMOUNTABLE state.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMNOTMOuntablename--location---------------------------><
```

Parameters

location (Required)
Specifies the name of the onsite location for storing the media. The name can be up to 255 characters. Enclose the name in quotation marks if it contains any blank characters.

Example: Specify the name of the onsite location

Set the name of the location to room 123/31.

```
set drmnotmountablename "room 123/31"
```

Related commands

Table 1. Commands related to SET DRMNOTMOUNTABLENAME

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMPLANPREFIX (Specify a prefix for recovery plan file names)

Use this command to specify a prefix for a recovery plan file name.

If you issue this command, IBM Spectrum Protect™ uses the specified prefix if the PREPARE command does not include the PLANPREFIX parameter.

Use the QUERY DRMSTATUS command to display the current value for the recovery plan prefix.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMPLANPrefix--prefix-----------------------------------><
```

Parameters

AIX Linux prefix (Required)

AIX Linux Specifies the prefix for a recovery plan file name. The maximum length of the prefix is 250 characters. If you enter a null string (""), the current prefix is removed, and the server uses the algorithm described in the PLANPREFIX parameter in the PREPARE command.
For the prefix, you can specify:

- **A directory path followed by a forward slash (/):** IBM Spectrum Protect appends to the prefix the date and time in the `yyyymmdd.hhmmss` format. For example, the SET DRMPLANPREFIX is set to the following:

  ```
  /adsmsrv/recplans/
  ```

  The resulting recovery plan file name is:

  ```
  /adsmsrv/recplans/19971115.051421
  ```

- **A directory path followed by a string:** IBM Spectrum Protect uses the string as part of the file name. IBM Spectrum Protect appends to the prefix the date and time in the `.yyyymmdd.hhmmss` format (note the initial period). For example, the SET DRMPLANPREFIX is set to the following:

  ```
  /adsmsrv/recplans/accounting
  ```

  The resulting recovery plan filename is:

  ```
  /adsmsrv/recplans/accounting.19971115.051421
  ```

- **A string that is not preceded by a directory path:** IBM Spectrum Protect appends to the prefix the date and time information in the `.yyyymmdd.hhmmss` format (note the initial period). IBM Spectrum Protect determines the directory path as follows:
  - IBM Spectrum Protect uses the directory path name of the current working directory of the IBM Spectrum Protect server. For example, the current IBM Spectrum Protect working directory is /opt/tivoli/tsm/server/binThe SET DRMPLANPREFIX command is set to the following:

    ```
    shipping
    ```

    The resulting recovery plan file name is:

    ```
    /opt/tivoli/tsm/server/bin/shipping.19971115.051421
    ```

Windows prefix (Required)

Windows Specifies a prefix for the path name used to generate the recovery plan file name. The prefix can be up to 200 characters. IBM Spectrum Protect uses the prefix if the PREPARE command is issued without the PLANPREFIX parameter. IBM Spectrum Protect builds a unique recovery plan file name by appending to the prefix the date and time format: `yyyymmdd.hhmmss` (for example, 19951115.051421). If you enter a null string (""), the current prefix is removed, and the server uses the algorithm described in the PLANPREFIX parameter in the PREPARE command.
For the prefix, you can specify:

1. A directory path
2. A directory path followed by a string
3. A string

The following describes the rules for possible prefix specifications:

1. To specify a directory path for the prefix, end the prefix with a back slash (\). IBM Spectrum Protect appends to the prefix the date and time information using the `yyyymmdd.hhmmss` format. For example the SET DRMPLANPREFIX is set to the following:

   ```
   c:\adsmsrv\recplans\
   ```

The resulting recovery plan file name is:

```
c:\adsmsrv\recplans\19951115.051421
```

Important: If you issue the SET DRMPLANPREFIX command from a command line client and the last character in the command line is a back slash, IBM Spectrum Protect interprets it as a continuation character. To avoid this, enclose the prefix in quotation marks. For example: `"c:\adsmsrv\recplans\"`

2. If the prefix is a directory path followed by a string, IBM Spectrum Protect uses the string as part of the file name. IBM Spectrum Protect appends to the prefix the date and time in the `.yyyymmdd.hhmmss` format (note the initial period). For example, the SET DRMPLANPREFIX is set to the following

   ```
   c:\adsmsrv\recplans\accounting
   ```

   The resulting recovery plan filename is the following:

   ```
   c:\adsmsrv\recplans\accounting.19951115.051421
   ```

3. If the prefix is a string that is not preceded by a directory path, IBM Spectrum Protect appends to the prefix the date and time information in the `.yyyymmdd.hhmmss` format (note the initial period). The directory path that IBM Spectrum Protect uses is the directory path representing this instance of the IBM Spectrum Protect server (typically the directory that the IBM Spectrum Protect server was originally installed from). For example, the directory representing this instance of the server is c:\Program Files\Tivoli\TSM;\server2, and you set the prefix to:

   ```
   shipping
   ```

   The resulting recovery plan filename is:

   ```
   c:\Program Files\Tivoli\TSM;\server2\shipping.19951115.051421
   ```

Example: Specify a prefix for recovery plan file names

Specify a prefix so that the generated recovery plan files are stored in the following directory:

- AIX Linux /drmplan/primsrv
- Windows c:\drmtest\prepare\

Issue the command: AIX Linux

```
set drmplanprefix /drmplan/primsrv/
```

Windows

```
set drmplanprefix c:\drmtest\prepare\
```

Related commands

Table 1. Commands related to SET DRMPLANPREFIX

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMPLANVPOSTFIX (Specify replacement volume names)

Use this command to specify the character to be appended to replacement volume names in the recovery plan file. The character can help you find or generate replacement volume names when you use the recovery plan file.

At installation, the character is set to @. IBM Spectrum Protect™ generates replacement names for primary storage pool volumes that were added by the DEFINE VOLUME command. Use the appended character to:

- Find replacement volume names in the recovery plan stanzas so that you can change the names at recovery time. For example, you may not know the names of the available tape volumes at the recovery site.
- Generate replacement volume names. You need a naming convention that works for any device type in your primary storage pools. Consider the following:
  - The generated length of replacement volume name
  - Legal characters in the replacement volume name

- Conflicts with existing volume names
- A replacement volume name must be different from any destroyed, existing, or new volume name.

Use the QUERY DRMSTATUS command to see the character added to the end of the replacement volume names.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMPLANVpostfix--character------------------------------><
```

Parameters

character (Required)

Specifies the character appended to the replacement volume names in the recovery plan file. Specify an alphanumeric or special character.

AIX Attention: A special character can cause unpredictable results in the AIX® shell or command line environment.

Windows Attention: A special character can cause unpredictable results in the Windows batch/command line environment.

Example: Specify the appended character for replacement volume names

Set the character appended to the replace volume names to R.

```
set drmplanvpostfix R
```

Related commands

Table 1. Commands related to SET DRMPLANVPOSTFIX

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMSTATUS	Displays DRM system parameters.

SET DRMPRIMSTGPOOL (Specify the primary storage pools to be managed by DRM)

Use this command to specify the names of primary storage pools that you want to recover. If the PREPARE command does not include the PRIMSTGPOOL parameter, DRM processes the names specified in this command.

Use the QUERY DRMSTATUS command to display the current settings. At installation, all primary storage pools defined to the server are eligible for DRM processing.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                      .-,-----------------.
                      V                   |
>>-Set DRMPRIMstgpool----primary_pool_name-+-------------------><
```

Parameters

primary_pool_name (Required)

Specifies the names of the primary storage pool names you want to recover. Separate multiple names with commas and no intervening spaces. You can use wildcard characters to specify names. The names that you specify replace any previous setting. If you enter a null string (""), all current names are removed, and all primary storage pools are eligible for DRM processing.

Example: Set a primary storage pool to be managed by DRM

Set the primary storage pool to be managed by DRM to PRIMSTGPOOL1.

```
set drmprimstgpool primstgpool1
```

Related commands

Table 1. Commands related to SET DRMPRIMSTGPOOL

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMSTATUS	Displays DRM system parameters.
SET DRMCOPYSTGPOOL	Specifies that copy storage pools are managed by DRM.

SET DRMRPFEXPIREDAYS (Set criteria for recovery plan file expiration)

Use this command to specify when recovery plan files are eligible for expiration. This command and expiration processing apply only to recovery plan files that were created with the DEVCLASS parameter specified on the PREPARE command (that is, virtual volumes of type RPFILE and RPSNAPSHOT). Expiration processing on the source server expires plan files that are stored on the target server. Locally created recovery plan files are not expired.

An RPFILE file is associated with a full plus incremental database backup series. An RPFSNAPSHOT file is associated with a database snapshot backup series.

Attention: The latest RPFILE and RPFSNAPSHOT files are never deleted.
A recovery plan file is eligible for expiration if both of the following are true:

- The last recovery plan file of the series exceeds the expiration value that is specified with the SET DRMRPFEXPIREDAYS command and the value that is specified for the DELgraceperiod parameter in the DEFINE SERVER command. The default value for the DELgraceperiod parameter is 5 days. For example, if you set the value for the SET DRMRPFEXPIREDAYS command to 80 days and set the value for the DELgraceperiod parameter to 6 days, the recovery plan file does not expire until 86 days elapse.
- The latest recovery plan file is not associated with the most recent database backup series.

For more information about expiration processing, see the EXPIRE INVENTORY command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set DRMRPFEXpiredays--days---------------------------------><
```

Parameters

days (Required)
Specifies the number of days that must elapse before a recovery plan file expires. You can specify a number 0 - 9999. At installation, this value is set to 60.

Example: Set the recovery plan expiration

Set the recovery plan file expiration value to 30.

```
set drmrpfexpiredays 30
```

Related commands

Table 1. Commands related to SET DRMRPFEXPIREDAYS

Command	Description
PREPARE	Creates a recovery plan file.
QUERY DRMSTATUS	Displays DRM system parameters.
QUERY RPFCONTENT	Displays the contents of a recovery plan file.
QUERY RPFILE	Displays information about recovery plan files.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.
DEFINE SERVER	Defines a server for server-to-server communications.

SET DRMVAULTNAME (Specify the vault name)

Use this command to specify the vault name. At installation the name is set to VAULT. Use the QUERY DRMSTATUS command to see the name of the vault.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET DRMVAultname--vault_name-------------------------------><
```

Parameters

vault_name (Required)
: Specifies the name of the vault. The name can be up to 255 characters. Enclose the name in quotation marks if it contains any blank characters.

Example: Specify a vault name

Specify `ironmountain` as the vault name.

```
set drmvaultname ironmountain
```

Related commands

Table 1. Commands related to SET DRMVAULTNAME

Command	Description
MOVE DRMEDIA	Moves DRM media onsite and offsite.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY DRMSTATUS	Displays DRM system parameters.

SET EVENTRETENTION (Set the retention period for event records)

Use this command to set the retention period for event records in the server database that will allow you to monitor completed schedules. An event record is created whenever processing of a scheduled command is started or missed.

You can adjust the length of time that the server maintains event information to avoid insufficient or outdated data. The server automatically removes the event records from the database after the retention period passes and the startup window for the event has elapsed.

You can issue the QUERY EVENT command to display information about scheduled and completed events.

You can issue the DELETE EVENT command to delete event records regardless of whether their retention period has passed.

You can issue the QUERY STATUS command to display the value for the event retention period. At installation, this value is set to 10 days.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set EVentretention--days-----------------------------------><
```

Parameters

days (Required)
: The number of days that the database retains event records. You can specify an integer from 0 to 9999. A value of 0 indicates that only event records for the current day are retained.

Example: Set the retention period for event records

Set the retention period to 15 days.

```
set eventretention 15
```

Related commands

Table 1. Commands related to SET EVENTRETENTION

Command	Description
DELETE EVENT	Deletes event records before a specified date and time.
QUERY EVENT	Displays information about scheduled and completed events for selected clients.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET FAILOVERHLADDRESS (Set a failover high level address)

Use this command to specify the IP address that a client uses to connect to this server as the secondary replication server during failover, if the address is different from the IP address that is specified for the replication process.

You must specify the address of the server that is used if the high-level address (HLA) is different. This command is required only if you use separate dedicated networks for server-to-server communication and client access.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET FAILOVERHladdress--high_level_address------------------><
```

Parameters

high_level_address (Required)

Specifies a server HLA as a numeric dotted decimal name or a host name to use during failover. If you specify a host name, a server that can resolve the name to the dotted decimal format must be available.

To remove the failover IP address, issue the command without specifying a value.

Example: Set a failover high-level address

The name of the HLA that you want to set for failover operations on this server.

```
set failoverhladdress server1
```

Example: Remove a high-level address

To remove a high-level address for a failover server, issue the following command:

```
set failoverhladdress
```

Related commands

Table 1. Commands related to QUERY REPLSERVER

Command	Description
QUERY REPLSERVER (Query a replication server)	Displays information about replicating servers.
REMOVE REPLSERVER (Remove a replication server)	Removes a server from replication.

SET INVALIDPWLIMIT (Set the number of invalid logon attempts)

Use this command to set the number of invalid logon attempts that are allowed before a node is locked.

The SET INVALIDPWLIMIT command also applies to LDAP directory servers that store complex node passwords. LDAP directory servers can limit the number of invalid password attempts independent of the IBM Spectrum Protect™ server. You might not want to set up the LDAP directory server for invalid attempts for the IBM Spectrum Protect namespace if you use the SET INVALIDPWLIMIT command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set--INVALIDPwlimit--number---------------------------------><
```

Parameters

number (Required)

Specifies the number of invalid logon attempts allowed before a node is locked.

You can specify an integer from 0 to 9999. A value of 0 means that invalid logon attempts are not checked. A value of 1 means that if a user issues an invalid password one time, the node is locked by the server. The default is 0.

Important: If your password is authenticated with an LDAP directory server, it can be managed by the LDAP server and the IBM Spectrum Protect server. Not all IBM Spectrum Protect server commands affect passwords that authenticate with an LDAP server. For example, the SET PASSEXP and RESET PASSEXP commands do not affect passwords that authenticate with an LDAP directory server. You can manage your password features through the IBM Spectrum Protect server. If you issued the SET INVALIDPWLIMIT command, all IBM Spectrum Protect passwords are controlled by the limit that you set. If you configure the LDAP directory server to limit the number of invalid password attempts, a conflict might occur.

Example: Define the number of allowed invalid login attempts

Set the number of invalid logon attempts allowed.

```
set invalidpwlimit 6
```

Related commands

Table 1. Commands related to SET INVALIDPWLIMIT

Command	Description
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET MINPWLENGTH	Sets the minimum length for client passwords.

SET LDAPPASSWORD (Set the LDAP password for the server)

Use this command to define a password for the user or account ID that you specified by using the SET LDAPUSER command.

Requirement: You must define the LDAPURL option and issue the SET LDAPUSER command before you issue the SET LDAPPASSWORD command. If the LDAPURL option is not defined when you set the user password for the Lightweight Directory Access Protocol (LDAP) server, you must restart the IBM Spectrum Protect™ server after you define the LDAPURL option.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set LDAPPassword--ldap_user_password------------------------><
```

Parameters

ldap_user_password
: Specifies the password that the IBM Spectrum Protect server uses when it authenticates to the LDAP server. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters. If you have equal signs within your password, you must contain the whole password within quotation marks. You can use the following characters:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Example: Set an LDAP password

```
set ldappassword LdAp20&12PaSsWoRd
```

Example: Set an LDAP password that includes an equal sign

```
set ldappassword "LdAp=LastWoRd"
```

Related commands

Table 1. Commands related to SET LDAPPASSWORD

Command	Description
AUDIT LDAPDIRECTORY	Audit an IBM Spectrum Protect-controlled namespace on an LDAP directory server.
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET LDAPUSER	Sets the user who oversees the passwords and administrators on the LDAP directory server.

SET LDAPUSER (Specify an ID for an LDAP directory server)

Use this command to specify the ID of a user or account that can access a Lightweight Directory Access Protocol (LDAP) server.

The specified ID must have read access to the accounts on the LDAP server that are used for authentication. To modify LDAP IDs or reset passwords for LDAP IDs, the specified ID must have write authority for accounts on the LDAP server.

Tip: The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set LDAPUser--ldap_user_dn---------------------------------><
```

Parameters

ldap_user_dn
: Specifies the ID of a user or account that can access an LDAP server.

Example: Specify an administrative user ID for conducting operations on an LDAP server

To specify an administrator with a user ID of JACKSPRATT, who represents a US company that is named EXAMPLE, issue the following command:

```
set ldapuser JackSpratt@us.example.com
```

Related commands

Table 1. Commands related to SET LDAPUSER

Command	Description
AUDIT LDAPDIRECTORY	Audit an IBM Spectrum Protect-controlled namespace on an LDAP directory server.
SET DEFAULTAUTHENTICATION	Specifies the default password authentication method for any REGISTER NODE or REGISTER ADMIN commands.
SET LDAPPASSWORD	Sets the password for the LDAPUSER.

SET LICENSEAUDITPERIOD (Set license audit period)

Use this command to specify the period, in days, between automatic license audits performed by IBM Spectrum Protect™.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                              .-30---.
>>-Set--LICenseauditperiod--+------+---------------------------><
                              '-days-'
```

Parameters

days
: Specifies the number of days between automatic server license audits. This parameter is optional. The default value is 30. You can specify an integer from 1 to 30, inclusive.

Example: Specify a 14 day server license audit

Specify that the server audits licenses every 14 days.

```
set licenseauditperiod 14
```

Related commands

Table 1. Commands related to SET LICENSEAUDITPERIOD

Command	Description
AUDIT LICENSES	Verifies compliance with defined licenses.
QUERY AUDITOCCUPANCY	Displays the server storage utilization for a client node.
QUERY LICENSE	Displays information about licenses and audits.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER LICENSE	Registers a license with the IBM Spectrum Protect server.

SET MAXCMDRETRIES (Set the maximum number of command retries)

Use this command to set the maximum number of times that a scheduler on a client node can retry a failed, scheduled command.

You can use the command to override the maximum number of retries that are specified by the client node. A client's value is overridden only if the client is able to connect with the server.

This command is used with the SET RETRYPERIOD command to regulate the time and the number of retry attempts to rerun failed command.

You can issue the QUERY STATUS command to display the current retry value. At installation, IBM Spectrum Protect™ is configured so that each client determines its own retry value.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set MAXCMDRetries--+--------+-------------------------------><
                      '-number-'
```

Parameters

number

Specifies the maximum number of times the scheduler on a client node can retry a failed scheduled command. This parameter is optional.

The default is that each client determines its own value for this parameter. You can specify an integer from 0 to 9999. See the appropriate client documentation for more information on setting the maximum command retries from the client.

Example: Set the maximum number of command retries to 2

Retry, only twice, a failed attempt to process a scheduled command.

```
set maxcmdretries 2
```

Related commands

Table 1. Command related to SET MAXCMDRETRIES

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET RETRYPERIOD	Specifies the time between retry attempts by the client scheduler.

SET MAXSCHEDSESSIONS (Set maximum scheduled sessions)

Use this command to set the number of sessions that the server can use to process scheduled operations. This command specifies the maximum number of scheduled sessions as a percentage of the total number of available server sessions.

Limiting the number of sessions ensures that some are available for unscheduled operations, such as backup or archive. You can increase either the total number of sessions (with the MAXSESSIONS parameter) or the maximum percentage of scheduled sessions. Increasing the total number of sessions available, however, can affect server performance. Increasing the maximum percentage of scheduled sessions can reduce the sessions available for unscheduled operations.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set MAXSCHedsessions--percent------------------------------><
```

Parameters

percent (Required)
Specifies the percentage of total server sessions that can be used for scheduled operations. You can specify an integer from 0 to 100. The MAXSESSIONS parameter in the server options file determines the maximum number of total available server sessions.

If you set the maximum percentage of scheduled sessions to 0, no scheduled events can begin. If you set the maximum percentage of scheduled sessions to 100, the maximum number of scheduled sessions is the value of the MAXSESSIONS option.

Tip: If the maximum number of scheduled sessions do not coincide with the percentage that you set in the SET MAXSCHEDSESSIONS command, run the SET MAXSCHEDSESSIONS command again. Look in the MAXSESSIONS option and determine the number that is specified there. If the MAXSESSIONS option number changed and you did not issue the SET MAXSCHEDSESSIONS command since the change, the maximum number of scheduled sessions can change.

Set a maximum of 20 sessions for scheduled activities

The MAXSESSIONS option has a value of 80. If you want no more than 20 sessions to be available for scheduled activity, set the percentage to 25.

```
set maxschedsessions 25
```

Related commands

Table 1. Commands related to SET MAXSCHEDSESSIONS

Command	Description
QUERY OPTION	Displays information about server options.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET MINPWLENGTH (Set minimum password length)

Use this command to set the minimum length of a password.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                      .-8------.
>>-Set--MINPwlength--+--------+------------------------------><
                      '-length-'
```

Parameters

length (Required)
: Specifies the minimum length of a password. This parameter is optional. You can specify an integer in the range 1 - 64. The default value is 8.

Example: Set the minimum password length

Set the minimum password length to 12 characters.

```
set minpwlength 12
```

Related commands

Table 1. Commands related to SET MINPWLENGTH

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET INVALIDPWLIMIT	Sets the number of invalid logon attempts before a node is locked.

Related reference:
SET SERVERPASSWORD (Set password for server)
DEFINE SERVER (Define a server for server-to-server communications)
UPDATE SERVER (Update a server defined for server-to-server communications)
REGISTER ADMIN (Register an administrator ID)
UPDATE ADMIN (Update an administrator)
REGISTER NODE (Register a node)
UPDATE NODE (Update node attributes)
SET LDAPPASSWORD (Set the LDAP password for the server)
BACKUP DB (Back up the database)
SET DBRECOVERY (Set the device class for automatic backups)

SET MONITOREDSERVERGROUP (Set the group of monitored servers)

Use this command to set the group of servers that are being monitored for alerts and status. You can also use this command to change or remove the group of monitored servers.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set MONITOREDSERVERGroup--+------------+-------------------><
                             '-group_name-'
```

Parameters

group_name
: Specifies the IBM Spectrum Protect™ server group name that contains all monitored servers. You can remove a monitored server group name by issuing the command without specifying a value, or by specifying an empty value (""). Any existing monitoring for alerts and status from remote servers is ended.

Set the name of a monitored server group

Set the name of a monitored server group SUBS, by issuing the following command:

```
set monitoredservergroup subs
```

Remove the name of a monitored server group

Remove the monitored server group, by issuing the following command:

```
set monitoredservergroup
```

Related commands

Table 1. Commands related to SET MONITOREDSERVERGROUP

Command	Description
DEFINE SERVERGROUP (Define a server group)	Defines a new server group.
DEFINE GRPMEMBER (Add a server to a server group)	Defines a server as a member of a server group.
DELETE GRPMEMBER (Delete a server from a server group)	Deletes a server from a server group.
QUERY SERVERGROUP (Query a server group)	Displays information about server groups.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET MONITORINGADMIN (Set the name of the monitoring administrator)	Set the name of the monitoring administrator.

SET MONITORINGADMIN (Set the name of the monitoring administrator)

Use this command to set the name of the monitoring administrator that is used to connect to the servers in the monitored server group.

To display the name of the monitored server group, issue the QUERY MONITORSETTINGS command.

The administrator name that you specify must match the name of an existing administrator, otherwise the command fails.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set MONITORINGADMIN--+------------+-------------------------><
                        '-admin_name-'
```

Parameters

admin_name
: Specifies administrator names. You can remove names by issuing the command without specifying a value, or by specifying an empty value ("").

Set the monitoring administrator name

Set the name of the monitoring administrator to MONADMIN, by issuing the following command:

```
set monitoringadmin monadmin
```

Remove the monitoring administrator name

Remove the monitoring administrator, by issuing the following command:

```
set monitoringadmin ""
```

Related commands

Table 1. Commands related to SET MONITORINGADMIN

Command	Description
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET MONITOREDSERVERGROUP (Set the group of monitored servers)	Set the group of monitored servers.

SET NODEATRISKINTERVAL (Specifies at-risk mode for an individual node)

Use this command to adjust the at-risk evaluation mode for an individual node.

Privilege class

To issue this command, you must have system privilege, policy privilege for the domain to which the node is assigned, or client owner authority over the node.

Syntax

```
>>---Set NODEATRISKINTERVAL--node_name-------------------------->

>--TYPE--=--+-DEFAULT--------------------+---------------------><
            +-BYPASSED-------------------+
            '-CUSTOM--Interval--=--value-'
```

Parameters

node_name (Required)
: Specifies the name of the client node that you want to update.

TYPE (Required)
Specifies the at-risk evaluation type. Specify one of the following values:

DEFAULT
Specifies that the node is evaluated with the same interval that was specified for the nodes classification by the SET STATUSATRISKINTERVAL command. The value is either system or applications, or VM, and is determined by the status monitor.

For example, you can specify `TYPE = DEFAULT`, which allows the status monitor to go ahead and classify the node automatically. Then the interval that is used, is the interval that was defined for that classification by the SET STATUSATRISKINTERVAL command.

BYPASSED
Specifies that the node is not evaluated for at-risk status by the status monitor. The at risk status is also reported as bypassed to the Operations Center.

CUSTOM
Specifies that the node is evaluated with the specified interval, rather than the interval that was specified by the SET STATUSATRISKINTERVAL command.

Interval
Specifies the amount of time, in hours, between client backup activity before the status monitor considers the client to be at risk. You can specify an integer in the range 6 - 8808. You must specify this parameter when `TYPE = CUSTOM`. You do not specify this parameter when `TYPE = BYPASSED` or `TYPE = DEFAULT`. The interval value for all client types is set to 24 at server installation.

Set node name to use a custom 90 day at-risk interval

Set the at-risk interval for a node named *fred* to 90 days.

```
set nodeatriskinterval fred type=custom interval=2160
```

Bypass the at-risk interval evaluation

Bypass the at-risk interval checking for a node named *bob*.

```
set nodeatriskinterval bob type=bypassed
```

Related commands

Table 1. Commands related to set nodeatriskinterval

Command	Description
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET VMATRISKINTERVAL (Specifies the at-risk mode for an individual VM filespace)	Sets the at-risk mode for a VM filespace
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
QUERY NODE (Query nodes)	Displays partial or complete information about one or more clients.

Command	Description
QUERY FILESPACE (Query one or more file spaces)	Displays information about data in file spaces that belong to a client.

SET PASSEXP (Set password expiration date)

Use this command to set the expiration period for administrator and client node passwords. You can either set a common password expiration period for all administrators and client node passwords or selectively set password expiration periods.

Restriction: The SET PASSEXP command does not apply to passwords that authenticate with an LDAP directory server.

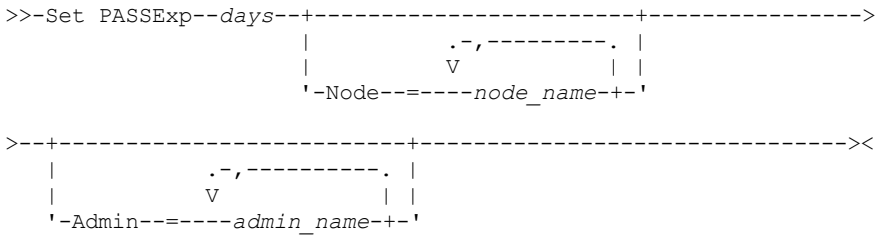
You can override the SET PASSEXP setting for one or more nodes by using the REGISTER NODE or UPDATE NODE command with the PASSEXP parameter.

The NODE or ADMIN parameters must be specified to change the password expiration period for client nodes or administrators with selectively set password expiration periods. If you do not specify the NODE or ADMIN parameters, *all* client node and administrator passwords will use the new password expiration period. If you selectively set a password expiration period for a client node or administrator that does not already have a set password expiration period, it is not modified if you later set a password expiration for all users.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

days (Required)
: Specifies the number of days that a password remains valid.

  You can specify from 1 to 9999 if you do not specify the NODE or the ADMIN parameter. If you specify the NODE or the ADMIN parameter, you can specify from 0 to 9999. A value of 0 means that the password never expires. If a password expires, the server prompts for a new password when the administrator or client node contacts the server.

Node
: Specifies the name of the node for which you are setting the password expiration period. To specify a list of nodes, separate the names with commas and no intervening spaces. This parameter is optional.

Admin
: Specifies the name of the administrator whose password expiration period you would like to set. To specify a list of administrators, separate the names with commas and no intervening spaces. This parameter is optional.

Example: Set the administrator and client node password expiration

Set the administrator and client node password expiration period to 45 days.

```
set passexp 45
```

Example: Set an administrator's password expiration

Set the administrator LARRY's password expiration period to 120 days.

```
set passexp 120 admin=larry
```

Related commands

Table 1. Commands related to SET PASSEXP

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER NODE	Defines a client node to the server and sets options for that user.
RESET PASSEXP	Resets the password expiration for nodes or administrators.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.
UPDATE NODE	Changes the attributes that are associated with a client node.

SET PRODUCTOFFERING (Set the product offering that is licensed to your enterprise)

Use the SET PRODUCTOFFERING command to define the IBM Spectrum Protect™ product offering that is licensed to your enterprise.

The definition is used to determine whether automatic storage capacity measurement calculations are required and made available for use by the IBM® License Metric Tool (ILMT). Run this command only if you are using ILMT to determine license consumption.

For product offerings where automatic storage capacity measurement calculations are made available for use by ILMT, the parameter also defines which capacity measurement approach is used for those calculations.

The capacity measurement approach is defined by the licensing terms of your specific product offering. To determine the currently calculated storage capacity for your product offering, see Verifying license compliance.

The same storage capacity information is made available to ILMT on a weekly interval. After an applicable product offering is defined by using this command, IBM Spectrum Protect makes the current capacity calculation for that offering available to the ILMT. After the initial capacity calculation is made available to ILMT, IBM Spectrum Protect updates the value weekly.

Privilege class

To run this command, you must have system privilege.

Syntax

```
>>-SET PRODUCTOFFERING--product_offering-----------------------><
```

Parameters

product_offering (Required)
Specifies a product offering. The maximum length of the text string is 255 characters. The following options are available:

ENTry
Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Entry. This product offering uses a Per Managed Server licensing metric. Capacity measurements for this product offering are not applicable.

DATARet
Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect for Data Retention. Capacity measurements for this product offering are not calculated automatically or made available for use by ILMT.

BASIC

Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect. This product offering uses a processor value unit (PVU) licensing metric. Capacity measurements for this product offering are not applicable.

EE
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Extended Edition. This product offering uses a PVU licensing metric. Capacity measurements for this product offering are not applicable.

SUIte
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITECloud
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite - IBM Cloud Object Storage Option. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITEEntry
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite Entry. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITEArchive
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite - Archive. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITEProtectier
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite - ProtecTier. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITEFrontend
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite - FrontEnd. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

SUITEENTRYFrontend
: Specifies that the product offering licensed in your enterprise is IBM Spectrum Protect Suite Entry - FrontEnd. Capacity measurements for this product offering are calculated automatically and made available for use by ILMT.

CLEAR
: No product offering is specified.

Example: Set the product offering to IBM Spectrum Protect (BASIC)

```
set productoffering BASIC
```

Related commands

Table 1. Commands related to SET PRODUCTOFFERING

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET QUERYSCHEDPERIOD (Set query period for polling client nodes)

Use this command to regulate how often client nodes contact the server to obtain scheduled work when it is running in the client-polling scheduling mode.

Each client can set its own retry period at the time its scheduler is started. You can use this command to override the value specified by all clients that can connect with the server.

If client nodes poll more frequently for schedules, the nodes receive changes to schedules more quickly. However, increased polling by the client nodes also increases network traffic.

You can issue the QUERY STATUS command to display the value for the period between schedule queries. At installation, IBM Spectrum Protect™ is configured so that each client node determines its own value for this setting.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set QUERYSCHedperiod--+-------+----------------------------><
                         '-hours-'
```

Parameters

hours
: Specifies the maximum number of hours the scheduler on a client node waits between attempts to contact the server to obtain a schedule. This parameter is optional. You can specify an integer from 1 to 9999. If you do not specify a value for this parameter, each client determines its own value for this parameter.

Example: Set the polling period for all client nodes

Have all clients using the polling scheduling mode contact the server every 24 hours.

```
set queryschedperiod 24
```

Related commands

Table 1. Commands related to SET QUERYSCHEDPERIOD

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET SCHEDMODES	Specifies the central scheduling mode for the server.

SET RANDOMIZE (Set randomization of scheduled start times)

Use this command to set randomized start times within the startup window of each schedule for clients by using the client-polling scheduling mode. A startup window is the start time and duration during which a schedule must be initiated. A client-polling scheduling mode is a client/server communication technique where the client queries the server for work.

Each schedule has a window during which it can be run. To balance network and server load, the start times for clients can be scattered across that window. Use this command to specify the fraction of the window over which start times for clients are distributed.

The randomization occurs at the beginning of the window to allow time for retries, if necessary. When the scheduling mode is not set to polling, randomization does not occur if the client's first contact with the server is after the start time for the event.

You can issue the QUERY STATUS command to display the value for the schedule randomization percentage. At installation, the value is 25 percent.

Set the randomization percentage to a value greater than 0 to prevent communication errors. Communication errors can result from a large group of clients contacting the server simultaneously. If you do experience communication errors, you can increase the randomization percentage so that client contact is spread out. This decreases the chance for communication overload and failure.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set RANDomize--percent--------------------------------------><
```

Parameters

percent (Required)

Specifies the percentage of the startup window over which the start times for individual clients are distributed. You can specify an integer from 0 to 50.

A value of 0 indicates that no randomization occurs and that all clients run schedules at the beginning of the startup windows.

A value of 50 indicates that clients are assigned start times that are randomly scattered across the first half of each startup window.

At installation, this value is 25, indicating that the first 25 percent of the window is used for randomization.

If you have specified DURUNITS=INDEFINITE in the DEFINE SCHEDULE command, the percentage is applied to a 24 hour period. For example, a value of 25 percent would result in a 6 hour window.

Example: Set randomization of scheduled start times

Set randomization to 50 percent.

```
set randomize 50
```

Related commands

Table 1. Commands related to SET RANDOMIZE

Command	Description
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET SCHEDMODES	Specifies the central scheduling mode for the server.

SET REPLRECOVERDAMAGED (Specify whether damaged files are recovered from a replication server)

Use this command to enable the system-wide recovery of damaged files from a target replication server. If this setting is turned on, the node replication process can be configured to detect damaged files on the source replication server and replace them with undamaged files from the target replication server.

The REPLRECOVERDAMAGED system parameter affects all file recovery processes across all replication processes for all nodes and file spaces. File recovery is possible only if the server software, Version 7.1.1 or later, is installed on the source and target replication servers, and if the node data was replicated before the file damage occurred.

To display the current setting, use the QUERY STATUS command.

When you install the server, the default setting is ON.

If you upgrade the server and no damaged files are detected, the default setting is ON.

If you upgrade the server and damaged files are detected, the parameter is set to OFF, and a message is issued to indicate that the recovery of damaged files is disabled. The OFF setting prevents the server from scanning database tables for damaged objects that can be recovered. Prevention of the scan is necessary in case many damaged files are detected. In that case, a scan can take a considerable amount of time, and should be scheduled when use of server resources is at a minimum. When you are ready to start the scan and recover damaged files, you must issue the SET REPLRECOVERDAMAGED command and specify the ON setting. After the server successfully completes the scan, the REPLRECOVERDAMAGED system parameter is set to ON.

The following table describes how the REPLRECOVERDAMAGED system parameter and other parameters affect the recovery of damaged, replicated files.

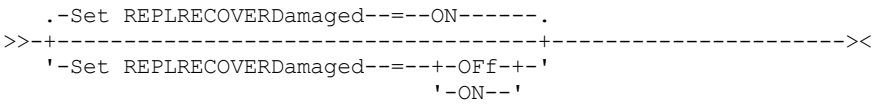
Table 1. Settings that affect the recovery of damaged files

Setting for the REPLRECOVERDAMAGED system parameter	Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command	Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands	Result
OFF	YES, NO, or not specified	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
OFF	ONLY	YES or NO	An error message is displayed because files cannot be recovered when the REPLRECOVERDAMAGED system parameter is set to OFF.
ON	YES	YES or NO	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	NO	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
ON	ONLY	YES or NO	Damaged files are recovered from the target replication server, but standard node replication does not occur.
ON	Not specified	YES	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	Not specified	NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

ON
: Specifies that node replication is enabled to recover damaged files from a target replication server.

OFf
: Specifies that node replication is not enabled to recover damaged files from a target replication server.

Example: Enable recovery of damaged files

To specify a system-wide setting that enables the server to recover damaged files from a target replication server, issue the following command:

```
set replrecoverdamaged on
```

Related commands

Table 2. Commands related to SET REPLRECOVERDAMAGED

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
UPDATE NODE	Changes the attributes that are associated with a client node.

SET REPLRETENTION (Set the retention period for replication records)

To maintain adequate information about replication processes, you can use this command to adjust the length of time that the source replication server retains replication records in its database. The SET REPLRETENTION command specifies the retention period for client-node replication records in the source replication-server database. You can use client node replication records to monitor running and completed processes.

A replication record is created when REPLICATE NODE command processing is started. By default, IBM Spectrum Protect™ retains client-node replication records for 30 calendar days. A calendar day consists of 24 hours, from midnight to midnight. For example, suppose that the retention period is two calendar days. If a replication process completes at 11:00 p.m. on day *n*, a record of that process is retained for 25 hours until midnight on day *n+1*. To display the retention period for replication records, issue the QUERY STATUS command on the source replication server.

Issue the SET REPLRETENTION command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
                      .-30-------------.
>>-Set REPLRETention--+----------------+----------------------><
                      '-number_of_days-'
```

Parameters

number_of_days (Required)

The number of days that the source replication server retains replication records. You can specify an integer 0 - 9999. The default value is 30.

Example: Set a retention period for client-node replication records

You want to retain client-node replication records for 10 days.

```
set replretention 10
```

Related commands

Table 1. Commands related to SET REPLRETENTION

Command	Description
QUERY REPLICATION	Displays information about node replication processes.

Command	Description
QUERY REPLNODE	Displays information about the replication status of a client node.
QUERY REPLRULE	Displays information about node replication rules.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET REPLSERVER (Set the target replication server)

Use this command to set the name of a target replication server. You can also use this command to change or remove a target replication server.

Issue this command on the server that acts as a source for replicated data.

To display the name of a target replication server, issue the QUERY STATUS command on a source replication server.

Important:

- The server name that you specify with this command must match the name of an existing server definition. It must also be the name of the server to be used as the target replication server. If the server name specified by this command does not match the server name of an existing server definition, the command fails.
- Use care when you are changing or removing a target replication server. If you change a target replication server, replicated client-node data is sent to a different target replication server. If you remove a target replication server, client node data is not replicated.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set REPLSERVer--+--------------------+----------------------><
                   '-target_server_name-'
```

Parameters

target_server_name

Specifies the name of the target replication server. The name that you specify must match the name of an existing server. The maximum length of a name is 64 characters.

To remove a target replication server, issue the command without specifying a value.
Note: If you do not want to continue replicating data, you can remove the node replication configuration after you remove the target replication server.

Example: Set a target replication server

The name of the server that you want to set as the target replication server is SERVER1.

```
set replserver server1
```

Related commands

Table 1. Commands related to SET REPLSERVER

Command	Description
DEFINE SERVER	Defines a server for server-to-server communications.

Command	Description
QUERY SERVER	Displays information about servers.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
UPDATE SERVER	Updates information about a server.
REMOVE REPLNODE	Removes a node from replication.
REMOVE REPLSERVER	Removes a server from replication.

SET RETRYPERIOD (Set time between retry attempts)

Use this command to set the number of minutes the scheduler on a client node waits between retry attempts after a failed attempt to contact the server or after a scheduled command fails to process.

Each client can set its own retry period at the time its scheduler program is started. You can use this command to override the values specified by all clients that can connect with the server.

This command is used in conjunction with the SET MAXCMDRETRIES command to regulate the period of time and the number of retry attempts to run a failed command.

You can issue the QUERY STATUS command to display the value for the period between retries. At installation, IBM Spectrum Protect™ allows each client to determine its own retry period.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set RETRYPeriod--+---------+--------------------------------><
                    '-minutes-'
```

Parameters

minutes
: Specifies the number of minutes the scheduler on a client node waits between retry attempts after a failed attempt to contact the server or after a scheduled command fails to process. When setting the retry period, set a time period that permits more than one retry attempt within a typical startup window. You can specify an integer from 1 to 9999.

Example: Set a fifteen minute time period between retry attempts

Have the client scheduler retry failed attempts to contact the server or to process scheduled commands every fifteen minutes.

```
set retryperiod 15
```

Related commands

Table 1. Commands related to SET RETRYPERIOD

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET MAXCMDRETRIES	Specifies the maximum number of retries after a failed attempt to execute a scheduled command.

SET SCHEDMODES (Select a central scheduling mode)

Use this command to determine how the clients communicate with the server to begin scheduled work. You must configure each client to select the scheduling mode in which it operates.

Use this command with the SET RETRYPERIOD command to regulate the time and the number of retry attempts to process a failed command.

You can issue the QUERY STATUS command to display the value for the scheduling mode supported. At installation, this value is ANY.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SCHEDMODes--+-ANY------+--------------------------------><
                   +-POlling--+
                   '-PRompted-'
```

Parameters

ANY
: Specifies that clients can run in either the client-polling or the server-prompted scheduling mode.

POlling
: Specifies that only the client-polling mode can be used. Client nodes poll the server at prescribed time intervals to obtain scheduled work.

PRompted
: Specifies that only the server-prompted mode can be used. This mode is only available for clients that communicate with TCP/IP. Client nodes wait to be contacted by the server when scheduled work needs to be performed and a session is available.

Example: Restrict scheduled operations to clients using client-polling

Clients can run under both server-prompted and client-polling central scheduling. You want to temporarily restrict the scheduled operations to clients that use the client-polling mode. If you set the schedule mode to POLLING, the server discontinues prompting clients to run scheduled commands. This means that any client scheduler using the server-prompted mode waits until you set the schedule mode to ANY or PROMPTED.

```
set schedmodes polling
```

Related commands

Table 1. Command related to SET SCHEDMODES

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET RETRYPERIOD	Specifies the time between retry attempts by the client scheduler.

SET SCRATCHPADRETENTION (Set scratch pad retention time)

Use this command to set the amount of time for which scratch pad entries are retained.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SET SCRATCHPADRETENTION--days-------------------------------><
```

Parameters

days (Required)
: Specifies the number of days that a scratchpad entry is retained after the last update to the scratchpad entry. You can enter an integer in the range 1 - 9999.

Example: Retain scratch pad entries for 367 days after they are updated

```
set scratchpadretention 367
```

Related commands

Table 1. Commands related to SET SCRATCHPADRETENTION

Command	Description
DEFINE SCRATCHPADENTRY	Creates a line of data in the scratch pad.
DELETE SCRATCHPADENTRY	Deletes a line of data from the scratch pad.
QUERY SCRATCHPADENTRY	Displays information that is contained in the scratch pad.
UPDATE SCRATCHPADENTRY	Updates data on a line in the scratch pad.

SET SERVERHLADDRESS (Set the high-level address of a server)

Use this command to set the high-level address (IP) of a server. IBM Spectrum Protect™ uses the address when you issue a DEFINE SERVER command with CROSSDEFINE=YES. You must use the SET SERVERHLADDRESS command for all automatic client deployments.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SERVERHladdress--ip_address----------------------------><
```

Parameters

ip_address (Required)
: Specifies a server high-level address as a numeric dotted decimal name or a host name. If a host name is specified, a server that can resolve the name to the dotted decimal form must be available.

Example: Set the high-level address of a server

Set the high-level address of HQ_SERVER to 9.230.99.66.

```
set serverhladdress 9.230.99.66
```

Related commands

Table 1. Command related to SET SERVERHLADDRESS

Command	Description
SET CROSSDEFINE	Specifies whether to cross define servers.
SET SERVERLLADDRESS	Specifies the low-level address of a server.

Command	Description
SET SERVERPASSWORD	Specifies the server password.

SET SERVERLLADDRESS (Set the low-level address of a server)

Use this command to set the low-level address of a server. IBM Spectrum Protect™ uses the address when you issue a DEFINE SERVER command with CROSSDEFINE=YES.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SERVERLladdress--tcp_port------------------------------><
```

Parameters

tcp_port (Required)
: Specifies the low-level address of the server. Generally, this address is identical to the TCPPORT option in the server option file of the server.

Example: Set the low-level address of a server

Set the low-level address of HQ_SERVER to 1500.

```
set serverlladdress 1500
```

Related commands

Table 1. Command related to SET SERVERLLADDRESS

Command	Description
SET CROSSDEFINE	Specifies whether to cross define servers.
SET SERVERHLADDRESS	Specifies the high-level address of a server.
SET SERVERPASSWORD	Specifies the server password.

SET SERVERNAME (Specify the server name)

Use this command to change the server name. When you install the IBM Spectrum Protect™ server, the name is set at installation to SERVER1.

Use the QUERY STATUS command to display the server name.

If you migrate from ADSM to IBM Spectrum Protect, the name is set to ADSM or the name last specified to ADSM with a SET SERVERNAME command.

Important:

- If this is a source server for a virtual volume operation, changing its name can impact its ability to access and manage the data it has stored on the corresponding target server.
- To prevent problems related to volume ownership, do not change the name of a server if it is a library client.

When changing the name of a server, be aware of the following additional restrictions:

- Windows clients use the server name to identify which passwords belong to which servers. Changing the server name after the clients are connected forces the clients to reenter the passwords.

- You must set unique names on servers that communicate with each other. On a network where clients connect to multiple servers, it is recommended that all of the servers have unique names.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SERVername--server_name---------------------------------><
```

Parameters

server_name (Required)
: Specifies the new server name. The name must be unique across a server network for enterprise event logging, enterprise configuration, command routing, or virtual volumes. The maximum length of the name is 64 characters.

Example: Name the server

Name the server WELLS_DESIGN_DEPT.

```
set servername wells_design_dept
```

Related commands

Table 1. Command related to SET SERVERNAME

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET SERVERPASSWORD (Set password for server)

Use this command to set the password for communication between servers to support enterprise administration and enterprise event logging and monitoring.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SERVERPAssword--password-------------------------------><
```

Parameters

password (Required)
: Specifies a password for the server. Other servers must have the same password in their definitions of this server. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

Example: Set a server password

Set the password for HQ_SERVER to agave234.

```
set serverpassword agave234
```

Related commands

Table 1. Command related to SET SERVERPASSWORD

Command	Description
SET CROSSDEFINE	Specifies whether to cross define servers.
SET SERVERHLADDRESS	Specifies the high-level address of a server.
SET SERVERLLADDRESS	Specifies the low-level address of a server.

SET SPREPLRULEDEFAULT (Set the server replication rule for space-managed data)

Use this command to set the server replication rule for space-managed data.

Restriction: The replication rule that you set with this command is applied only if file space rules and client node rules for space-managed data are set to DEFAULT.

Issue this command on the server that acts as a source for replicated data.

You can specify a normal-priority replication rule or a high-priority replication rule. In a replication process that includes both normal and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

For example, suppose that your client nodes contain space-managed data and backup data. Replication of the space-managed data is a higher priority than the backup data. To prioritize the space-managed data, issue the SET SPREPLRULEDEFAULT command and specify the ALL_DATA_HIGH_PRIORITY replication rule. To prioritize the backup data, issue the SET BKREPLRULEDEFAULT command and specify the ALL_DATA replication rule for backup data. The ALL_DATA rule for backup data replicates backup data with a normal priority.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SPREPLRuledefault--+-ALL_DATA----------------+----------><
                          +-ALL_DATA_HIGH_PRIORITY-+
                          '-NONE--------------------'
```

Parameters

ALL_DATA
: Replicates space-managed data with a normal priority.

ALL_DATA_HIGH_PRIORITY
: Replicates space-managed data with a high priority.

NONE
: Space-managed data is not replicated.

Example: Set the server replication rule for space-managed data

Set up the default rule for space-managed data to replicate with a high priority.

```
set spreplruledefault all_data_high_priority
```

Related commands

Table 1. Commands related to SET BKREPLRULEDEFAULT

Command	Description

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLRULE	Displays information about node replication rules.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET ARREPLRULEDEFAULT	Specifies the server node-replication rule for archive data.
SET BKREPLRULEDEFAULT	Specifies the server node-replication rule for backup data.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE REPLRULE	Enables or disables replication rules.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)

Use this command to adjust the backup activity interval that is used when the status monitor assesses whether clients are at risk.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>---Set STATUSATRISKINTERVAL--TYPE--=-----+-ALl----------+------>
                                           +-APplications-+
                                           +-VM-----------+
                                           '-SYstems------'

>----Interval--=--value-----------------------------------------><
```

Parameters

TYPE (Required)
: Specifies the type of client that should be evaluated. Specify one of the following values:

  ALl
  : Specify this setting for all client types.

  APplications
  : Specify this setting for only application client types.

  VM
  : Specify this setting for virtual system clients types.

  SYstems
  : Specify this setting for systems client types.

Interval (Required)
: Specifies the amount of time, in hours, between client activity before the status monitor considers the client to be at risk. You can specify an integer in the range 6 - 8808. The interval value for all client types is set to 24 at server installation.

Set systems to use a two-week at-risk interval

Set the at-risk interval check for systems client types to 2 weeks.

```
set statusriskinterval type=systems interval=336
```

Related commands

Table 1. Commands related to

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

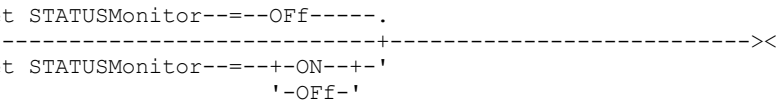
SET STATUSMONITOR (Specifies whether to enable status monitoring)

Use this command to enable and disable status monitoring. Turning status monitoring on for the first time also sets the default threshold values, and increases the event record retention to at least 14 days.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

ON

Specifies that the status monitoring is turned on. The first time that you set status monitoring to ON, it sets all the default threshold values that are specified in the DEFINE STATUSTHRESHOLD and UPDATE STATUSTHRESHOLD commands. It also sets the retention value for event records to at least 14 days. For example, when you turn status monitoring on, the default values for primary storage pool utilization is automatically set to display a warning when the threshold value reaches 80%, and an error when the threshold reaches 90% utilization.

OFF

Specifies that the status monitoring is turned off. Off is the default value.

Enable status monitoring

Set status monitoring to on to enable status monitoring.

```
set statusmonitor on
```

Related commands

Table 1. Commands related to SET STATUSMONITOR

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)

Use this command to specify the number of minutes between status monitoring server queries.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set STATUSREFreshinterval--minutes--------------------------><
```

Parameters

minutes (Required)

Specifies the approximate number of minutes between status monitoring server queries. You can specify an integer in the range 1 - 2440. The default value is 5.

Restrictions:

- In a storage environment that is monitored by the Operations Center, set the same refresh interval on the hub and spoke servers. If you use different intervals, the Operations Center can show inaccurate information for spoke servers.
- Short status refresh intervals use more space in the server database and might require more processor and disk resources. For example, decreasing the interval by half doubles the required database and archive log space. Long intervals reduce the currency of Operations Center data but better suit a high-latency network configuration.
- A status refresh interval of less than 5 minutes can cause the following issues:

- Operations Center data that is supposed to be refreshed after the defined interval takes a longer time to be refreshed.
- Operations Center data that is supposed to be refreshed almost immediately when a related change occurs in the storage environment also takes a longer time to be refreshed.

Set the refresh interval for status monitoring

Specify that the server status is queried every 6 minutes, by issuing the following command:

```
set statusrefreshinterval 6
```

Related commands

Table 1. Commands related to SET STATUSREFRESHINTERVAL

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)

Use this command to enable the status monitor to consider clients as at risk when evaluating the status for each client.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set STATUSSKIPASFAILURE--+-Yes-+----------------------------->
                            '-No--'

>--TYPE--=--+-ALl----------+----------------------------------><
            +-APplications-+
            +-VM-----------+
            '-SYstems------'
```

Parameters

State (Required)
Specifies whether to enable the check for skipped files during the last backup. This check signifies that the client is at-risk if any files were skipped. Client data that is skipped or not backed up properly is considered at risk.

Yes
Specifies that the server evaluates whether a client is at risk.
No
Specifies that the server does not evaluate whether a client is at risk.

TYPE (Required)
Specifies the type of client that should be evaluated. Specify one of the following values:

ALl
Specify this setting for all client types.
APplications
Specify this setting for only application client types.
VM
Specify this setting for virtual system clients types.
SYstems
Specify this setting for systems client types.

Disable at-risk evaluation for virtual system client types

Disable the at-risk evaluation for virtual systems client types by issuing the following command:

```
set statusskipasfailure off type=vm
```

Related commands

Table 1. Commands related to SET STATUSSKIPASFAILURE

Command	Description
DEFINE STATUSTHRESHOLD (Define a status monitoring threshold)	Defines a status monitoring threshold.
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

SET SUBFILE (Set subfile backup for client nodes)

Use this command to set up the server to allow clients to back up subfiles. On the client's workstation, the SUBFILECACHEPATH and SUBFILECACHESIZE options must be specified in the client's options file (dsm.opt). If you are using a Windows client, you must also specify the SUBFILEBACKUP option.

With subfile backups, when a client's file has been previously backed up, any subsequent backups are typically made to the portion (a subfile) of the client's file that has changed, rather than the entire file.

Use the QUERY STATUS command to determine whether subfiles can be backed up to the server running this command.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SUBFILE--+-Client-+-------------------------------------><
                '-No-----'
```

Parameters

Client
: Specifies that the client node can determine whether to use subfile backup.

No
: Specifies that the subfile backups are not to be used. At installation, this value is set to No.

Example: Set subfile backup for client nodes

Allow the client node to backup subfiles on the server.

```
set subfile client
```

Related commands

Table 1. Command related to SET SUBFILE

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET SUMMARYRETENTION (Set number of days to keep data in activity summary table)

Use this command to specify the number of days to keep information in the SQL activity summary table.

The SQL activity summary table contains statistics about each client session and server processes. For a description of the information in the SQL activity summary table, issue the following command:

```
select colname, remarks from columns where tabname='SUMMARY'
```

Issue the QUERY STATUS command to display the number of days the information is kept. At installation, IBM Spectrum Protect™ allows each server to determine its own number of days for keeping information in the SQL activity summary table.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-Set SUMmaryretention--+------+-----------------------------><
                         '-days-'
```

Parameters

days

Specifies the number of days to keep information in the activity summary table. You can specify a number from 0 to 9999. A value of 0 means that information in the activity summary table is not kept. A value of 1 specifies to keep the activity summary table for the current day.

Example: Specify the number of days to keep information in the SQL activity summary table

Set the server to retain the activity summary table information for 15 days.

```
set summaryretention 15
```

Related commands

Table 1. Commands related to SET SUMMARYRETENTION

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
SET ACTLOGRETENTION	Specifies the number of days to retain log records in the activity log.
QUERY ACTLOG	Displays messages from the server activity log.
SELECT	Allows customized queries of the IBM Spectrum Protect database.

SET TAPEALERTMSG (Set tape alert messages on or off)

Use this command to allow the IBM Spectrum Protect™ server to log notification of diagnostic information from library and drive devices. At installation, this value is set to OFF. When enabled, the server can retrieve diagnostic information from a tape or library device and display it using ANR messages. When disabled, the server will not query a device for this information.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-Set TAPEAlertmsg--+-ON--+-----------------------------------><
                     '-OFf-'
```

Parameters

ON

Specifies that diagnostic information will be reported to the server.

OFf

Specifies that diagnostic information will not be reported to the server.

Example: Set tape alert messages on

Allow the server to receive diagnostic information messages.

```
set tapealertmsg on
```

Related commands

Table 1. Command related to SET TAPEALERTMSG

Command	Description

Command	Description
QUERY TAPEALERTMSG	Displays whether the server logs hardware diagnostic information.

SET TOCLOADRETENTION (Set load retention period for table of contents)

Use this command to specify the approximate number of minutes that unreferenced table of contents data will remain loaded in the server database.

During NDMP-controlled backup operations of NAS file systems, the server can optionally collect information about files and directories in the image and store this information in a table of contents within a storage pool. The web client can be used to examine files and directories in one or more file-system images by displaying entries from the table of contents data. The server loads the necessary table of contents data into a temporary database table.

Once the data have been loaded, the user can then select those files and directories to be restored. Because this database table is temporary, the data will only remain loaded for a specified time since the last reference to that data. At installation, the retention time is set to 120 minutes. Use the QUERY STATUS command to see the table of contents load retention time.

Privilege class

To issue this command you must have system privilege.

Syntax

```
>>-Set TOCLOADRetention--minutes------------------------------><
```

Parameters

minutes (Required)
: Specifies the approximate number of minutes that an unreferenced table of contents data is retained in the database. You can specify an integer from 30 to 1000.

Example: Define the load retention period for the table of contents

Use the command, SET TOCLOADRETENTION, to specify that unreferenced table of contents data is to be retained in the database for 45 minutes.

```
set tocloadretention 45
```

Related commands

Table 1. Commands related to SET TOCLOADRETENTION

Command	Description
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

SET VMATRISKINTERVAL (Specifies the at-risk mode for an individual VM filespace)

Use this command to adjust the at-risk evaluation mode for an individual VM filespace.

Privilege class

To issue this command, you must have system privilege, policy privilege for the domain to which the node is assigned, or client owner authority over the node.

Syntax

```
>>---Set VMATRISKINTERVAL--node_name--fsid---------------------->

>--TYPE--=--+-DEFAULT--+--+--------------------+--------------><
            +-BYPASSED-+  '-Interval--=--value-'
            '-CUSTOM---'
```

Parameters

node_name (Required)
: Specifies the name of the client node, that owns the VM filespace, that you want to update.

fsid (Required)
: Specifies the filespace ID of the client node that you want to update.

TYPE (Required)
: Specifies which at-risk evaluation mode the status monitor should use when evaluating the at-risk classification for the specified nodes VM filespace. Specify one of the following values:

  DEFAULT
  : Specifies that the VM filespace is evaluated with the same interval that was specified for the SET STATUSATRISKINTERVAL command.

  BYPASSED
  : Specifies that the VM filespace is not evaluated for at-risk status by the status monitor. The at-risk status is also reported as bypassed to the Operations Center.

  CUSTOM
  : Specifies that the VM filespace is evaluated with the specified interval, rather than the interval that was specified for the SET STATUSATRISKINTERVAL command.

Interval
: Specifies the amount of time, in hours, between client backup activity before the status monitor considers the client to be at risk. You can specify an integer in the range 6 - 8808. You must specify this parameter when `TYPE = CUSTOM`. You do not specify this parameter when `TYPE = BYPASSED` or `TYPE = DEFAULT`. The interval value for all client types is set to 24 at server installation.

Set node name to use a custom 90 day at-risk interval

Set the at-risk interval for a node named *charlievm* (filespace ID 50) on datacenter node named *alice* to use a 90 day at-risk interval. You can issue the QUERY FILESPACE command to determine the filespace ID for the VM.

```
set vmatriskinterval alice 50 type=custom interval=2160
```

Bypass the at-risk interval evaluation

Exclude the VM called *davevm* (filespace ID 213) on datacenter node named *erin* from at-risk interval checking. You can issue the QUERY FILESPACE command to determine the filespace ID for the VM called *davevm*. Then set the at-risk interval check for the VM as bypassed.

```
set vmatriskinterval erin 213 type=bypassed
```

Related commands

Table 1. Commands related to set vmatriskinterval

Command	Description
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET NODEATRISKINTERVAL (Specifies at-risk mode for an individual node)	Sets the at-risk mode and interval for a node

Command	Description
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
QUERY NODE (Query nodes)	Displays partial or complete information about one or more clients.
QUERY FILESPACE (Query one or more file spaces)	Displays information about data in file spaces that belong to a client.

SETOPT (Set a server option for dynamic update)

You can use the SETOPT command to update most server options dynamically without stopping and restarting the server. For the DBDIAGLOGSIZE option, you must stop and start the server. A SETOPT command contained in a macro or a script cannot be rolled back.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-SETOPT--option_name--option_value--------------------------><
```

Parameters

option_name (Required)

Specifies a text string of information identifying the server option to be updated. The maximum length of the text string is 255 characters. The following options are available:

- ADMINCOMMTimeout
- ADMINIDLETIMEOUT
- ALLOWREORGINDEX
- ALLOWREORGTABLE
- ARCHLOGCOMPress
- BACKUPINITIATIONROOT
- CHECKTAPEPOS
- CLIENTDEDUPTXNlimit
- CLIENTDEPLOYCATALOGURL
- CLIENTDEPLOYUSELOCALCATALOG
- COMMTimeout
- Windows DATEFORMAT
- DBDIAGLOGSize
- DBDIAGPATHFSTHreshold
- DEDUPTIER2FILESIZE
- DEDUPTIER3FILESIZE
- DEDUPREQUIRESBACKUP
- DNSLOOKUP
- EXPINterval

- EXPQUiet
- FSUSEDTHreshold
- IDLETimeout
- LDAPCACHEDURATION
- MAXSessions
- MOVEBatchsize
- MOVESizethresh
- NDMPPREFDATAINTERFACE
- Windows NUMBERFORMAT
- NUMOPENVOLSallowed
- RECLAIMDELAY
- RECLAIMPERIOD
- REORGBEGINTime
- REORGDURation
- RESOURCETimeout
- RESTOREINTERVAL
- RETENTIONEXTENSION
- AIX Linux Windows SANDISCOVERY
- AIX Linux Windows SANREFRESHTIME
- SERVERDEDUPTXNlimit
- SHREDding
- Windows TCPPORT
- THROUGHPUTDatathreshold
- THROUGHPUTTimethreshold
- Windows TIMEFORMAT
- TXNGroupmax

option_value (Required)
Specifies the value for the server option.

Example: Set the maximum number of client sessions

Update the server option for the maximum number of client sessions to a value of 40.

```
setopt maxsessions 40
```

Related commands

Table 1. Commands related to SETOPT

Command	Description
QUERY OPTION	Displays information about server options.
QUERY SYSTEM	Displays details about the IBM Spectrum ProtectIBM Spectrum Protect™ server system.

SHRED DATA (Shred data)

Use this command to manually start the process of shredding deleted sensitive data. Manual shredding is possible only if automatic shredding is disabled.

You can control automatic shred processing with the SHREDDING server option.

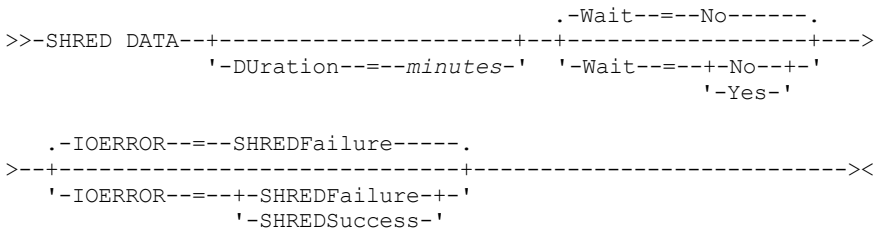
This command creates a background process that can be canceled with the CANCEL PROCESS command. To display information on background processes, use the QUERY PROCESS command.

If data from a storage pool that enforces shredding is deleted while a manual shredding process is running, it will be added to the running process.

Privilege class

To issue this command you must have system privilege.

Syntax



Parameters

DURATION
: Specifies the maximum number of minutes the shredding process runs before being automatically canceled. When the specified number of minutes elapses, the server cancels the shredding process. As soon as the process recognizes the cancellation, it ends. Because of this, the process may run longer than the value you specified for this parameter. You can specify a number from 1 to 9999. This parameter is optional. If not specified, the server will stop only after all deleted sensitive data has been shredded.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is No. Possible values are:

  No
  : Specifies that the server processes this command in the background. You can continue with other tasks while the command is being processed. Messages created from the background process are displayed either in the activity log or the server console, or both, depending on where messages are logged. To cancel a background process, use the CANCEL PROCESS command. If you cancel this process, some files might already have been shredded before the cancellation. This is the default.

  Yes
  : Specifies that the server processes this command in the foreground. You must wait for the operation to complete before continuing with other tasks. The server displays the output messages to the administrative client when the operation completes. Messages are also displayed either in the activity log or the server console, or both, depending on where messages are logged.
  AIX Linux Note: You cannot specify WAIT=YES from the server console.

IOERROR
: Specifies whether an I/O error encountered while shredding the data is to be considered a successful shred. This parameter is optional. The default is SHREDFAILURE. Possible values are:

  SHREDFailure
  : Specifies that if the server encounters an I/O error while shredding, the data will not be considered successfully shredded and the owning file will be marked as damaged. The server will attempt to shred the data again the next time the shredding process runs, giving you a chance to correct the error and ensure the data can be properly shredded.

  SHREDSuccess
  : Specifies that if the server encounters an I/O error while shredding and the owning file had been previously marked as damaged, the data will be considered successfully shredded. You should use this option only after the server has reported I/O errors while shredding and you are unable to correct the error.

Example: Shred data

Manually start the shredding of all deleted sensitive data. Continue the process for up to six hours before automatically canceling it.

```
shred data duration=360
```

Related commands

Table 1. Commands related to SHRED DATA

Command	Description

Command	Description
CANCEL PROCESS	Cancels a background server process.
QUERY PROCESS	Displays information about background processes.
QUERY SHREDSTATUS	Displays information about data waiting to be shredded.

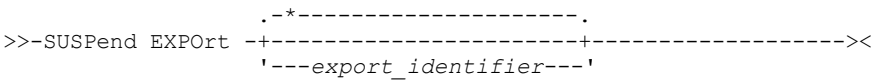
SUSPEND EXPORT (Suspend a currently running export operation)

Use this command to suspend a currently running server-to-server export operation which has a FILEDATA value that is not NONE. The export operation that you want to suspend must be past the initialization phase to be eligible for suspension. The state of the export operation is saved. The operation can be restarted by issuing the RESTART EXPORT command.

Privilege class

You must have system privilege to issue this command.

Syntax



Parameters

EXPORTIDentifier
: This optional parameter specifies the name of the export operation. You can find a name by issuing the QUERY EXPORT command to list all the currently running server-to-server export operations that can be suspended. You can also use the wildcard character to specify the name.

Example: Suspend a specific export operation

Suspend the running export operation EXPORTALLACCTNODES. No output is generated when you issue the SUSPEND EXPORT command. You must issue the QUERY EXPORT command to verify that the EXPORTALLACCTNODES operation is suspended.

```
suspend export exportallacctnodes
```

Example: Suspend all running export operations

Suspend all the export operations with a state of RUNNING.

```
suspend export *
```

Related commands

Table 1. Commands related to SUSPEND EXPORT

Command	Description
CANCEL EXPORT	Deletes a suspended export operation.
EXPORT NODE	Copies client node information to external media or directly to another server.
EXPORT SERVER	Copies all or part of the server to external media or directly to another server.
QUERY EXPORT	Displays the export operations that are currently running or suspended.
RESTART EXPORT	Restarts a suspended export operation.

UNLOCK commands

Use the UNLOCK commands to reestablish access after an object was locked.

- UNLOCK ADMIN (Unlock an administrator)
- UNLOCK NODE (Unlock a client node)
- UNLOCK PROFILE (Unlock a profile)

UNLOCK ADMIN (Unlock an administrator)

Use the UNLOCK ADMIN command to allow a locked administrator to access the server again. You can also unlock multiple administrators that authenticate with the same method.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UNLOCK Admin--+-*----------+--+-------------------------------+->< 
                 '-admin_name-'  '-AUTHentication--=--+-LOcal-+-'
                                                      '-LDap--'
```

Parameters

admin_name (Required)
: Specifies the name of the administrator to unlock. You can use wildcard characters to specify the administrator name. You do not have to enter an administrator name if you want to unlock all of the administrators according to their method of authentication. Use the wildcard with an authentication method to unlock multiple administrators. The parameter is required (no default wildcard).

AUTHentication
: Specifies the method of password authentication that is needed for an administrator to log on.

  LOcal
  : Specifies that you want to unlock administrator user IDs that authenticate passwords with the IBM Spectrum Protect™ server.

  LDap
  : Specifies that you want to unlock administrator user IDs that authenticate passwords with an LDAP directory server.

Example: Unlock an administrator user ID

The administrator user ID JOE is locked out of IBM Spectrum Protect. Allow JOE to access the server. Issue the following command:

```
unlock admin joe
```

Example: Unlock all administrator user IDs that authenticate passwords with an LDAP directory server

The administrator user ID that use passwords that authenticate with an LDAP directory server must be unlocked so the IDs can communicate with the IBM Spectrum Protect server.

```
unlock admin * authentication=ldap
```

Related commands

Table 1. Commands related to UNLOCK ADMIN

Command	Description

Command	Description
LOCK ADMIN	Prevents an administrator from accessing IBM Spectrum Protect.
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.

UNLOCK NODE (Unlock a client node)

Use this command to allow a locked client node to access the server again. You can also unlock multiple nodes that use the same method of authentication.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax

```
>>-UNLOCK Node--+-*---------+--+-------------------------------+-><
               '-node_name-'  '-AUTHentication--=--+-LOcal-+-'
                                                   '-LDap--'
```

Parameters

node_name (Required)
: Specifies the name of the client node to unlock. You can use wildcard characters to specify the node name. You do not have to enter a node name if you want to unlock all of the nodes according to their method of authentication. Use the wildcard with an authentication method to unlock groups of nodes. The parameter is required. There is no default wildcard character available.

AUTHentication
: Specifies the node password authentication method. This parameter is optional.

  LOcal
  : Specifies that you want to unlock nodes that authenticate passwords with the IBM Spectrum Protect™ server.

  LDap
  : Specifies that you want to unlock nodes that authenticate passwords with an LDAP directory server.

Example: Unlock a node

The client node SMITH is locked out of IBM Spectrum Protect. Allow SMITH to access the server.

```
unlock node smith
```

Example: Unlock all nodes that authenticate with the IBM Spectrum Protect server

The nodes that are not authenticating passwords with LDAP directory servers must be unlocked.

```
unlock node * authentication=local
```

Related commands

Table 1. Commands related to UNLOCK NODE

Command	Description
LOCK NODE	Prevents a client from accessing the server.
QUERY NODE	Displays partial or complete information about one or more clients.

UNLOCK PROFILE (Unlock a profile)

Use this command on a configuration manager to unlock a configuration profile so it can be distributed to subscribing managed servers.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UNLOCK PROFIle--profile_name--------------------------------><
```

Parameters

profile_name (Required)
Specifies the profile to unlock. You can use wildcard characters to indicate multiple names.

Example: Unlock a profile

Unlock a profile named TOM.

```
unlock profile tom
```

Related commands

Table 1. Commands related to UNLOCK PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UPDATE PROFILE	Changes the description of a profile.

UPDATE commands

Use the UPDATE command to modify one or more attributes of an existing IBM Spectrum Protect™ object.

- UPDATE ADMIN (Update an administrator)
- UPDATE ALERTTRIGGER (Update a defined alert trigger)
- UPDATE ALERTSTATUS (Update the status of an alert)
- UPDATE BACKUPSET (Update a retention value assigned to a backup set)
- UPDATE CLIENTOPT (Update a client option sequence number)
- UPDATE CLOPTSET (Update a client option set description)
- UPDATE COLLOCGROUP (Update a collocation group)
- UPDATE COPYGROUP (Update a copy group)
- UPDATE DATAMOVER (Update a data mover)
- UPDATE DEVCLASS (Update the attributes of a device class)
- UPDATE DOMAIN (Update a policy domain)

- UPDATE DRIVE (Update a drive)
- UPDATE FILESPACE (Update file-space node-replication rules)
- UPDATE LIBRARY (Update a library)
- UPDATE LIBVOLUME (Change the status of a storage volume)
- UPDATE MACHINE (Update machine information)
- UPDATE MGMTCLASS (Update a management class)
- UPDATE NODE (Update node attributes)
- UPDATE NODEGROUP (Update a node group)
- UPDATE PATH (Change a path)
- UPDATE POLICYSET (Update a policy set description)
- UPDATE PROFILE (Update a profile description)
- UPDATE RECOVERYMEDIA (Update recovery media)
- UPDATE REPLRULE (Update replication rules)
- UPDATE SCHEDULE (Update a schedule)
- UPDATE SCRIPT (Update an IBM Spectrum Protect script)
- UPDATE SERVER (Update a server defined for server-to-server communications)
- UPDATE SERVERGROUP (Update a server group description)
- UPDATE SPACETRIGGER (Update the space triggers)
- UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)
- UPDATE STGRULE (Update a storage rule for tiering)
- UPDATE STGPOOL (Update a storage pool)
- AIX Linux Windows UPDATE STGPOOLDIRECTORY (Update a storage pool directory)
- UPDATE VIRTUALFSMAPPING (Update a virtual file space mapping)
- UPDATE VOLHISTORY (Update sequential volume history information)
- UPDATE VOLUME (Change a storage pool volume)

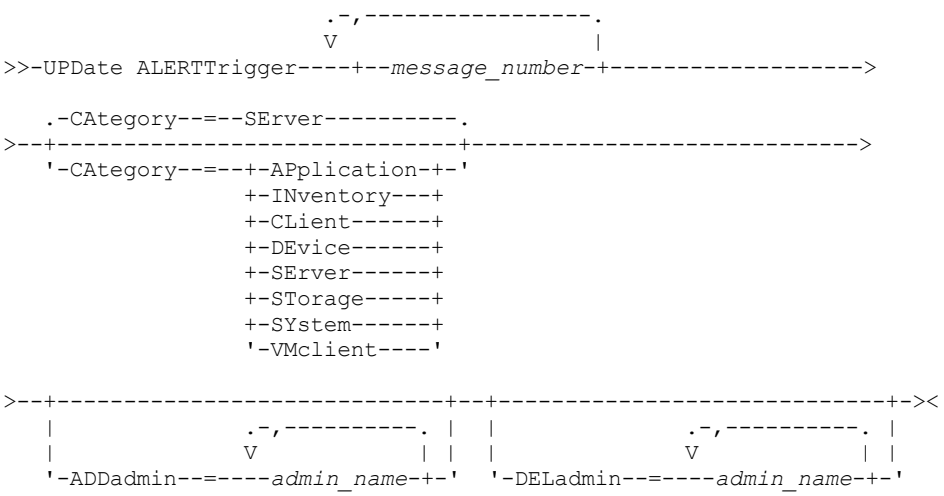
UPDATE ALERTTRIGGER (Update a defined alert trigger)

Use this command to update the attributes of one or more alert triggers.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

message_number (Required)
: Specifies the message number that you want to associate with the alert trigger. Specify multiple message numbers, which are separated by commas, and no intervening spaces. Message numbers are a maximum of eight characters in length.

CATegory

Specifies the category type for the alert, which is determined by the message types. The default value is SERVER.
Note: Changing the category of an alert trigger does not change the category of existing alerts on the server. New alerts are categorized with the new category.
Specify one of the following values:

APplication
: Alert is classified as application category. For example, you can specify this category for messages that are associated with application (TDP) clients.

INventory
: Alert is classified as inventory category. For example, you can specify this category for messages that are associated with the database, active log file, or archive log file.

CLient
: Alert is classified as client category. For example, you can specify this category for messages that are associated with general client activities.

DEvice
: Alert is classified as device category. For example, you can specify this category for messages that are associated with device classes, libraries, drives, or paths.

SErver
: Alert is classified as general server category. For example, you can specify this category for messages that are associated with general server activities or events.

STorage
: Alert is classified as storage category. For example, you can specify this category for messages that are associated with storage pools.

SYstems
: Alert is classified under system clients category. For example, you can specify this category for messages that are associated with system backup and archive or hierarchical storage management (HSM) backup-archive clients.

VMclient
: Alert is classified under VMclient category. For example, you can specify this category for messages that are associated with virtual machine clients.

ADmin
: This optional parameter specifies the name of the administrator who receives email notification of this alert. The alert trigger is defined successfully even if no administrator names are specified.

ADDadmin
: Specifies the administrator name that you want to add to the list of administrators that receive email alerts. Specify multiple administrator names, which are separated by commas, and no intervening spaces.

DELadmin
: Specifies the administrator name that you want to delete from the list of administrators that receive email alerts. Specify multiple administrator names, which are separated by commas, and no intervening spaces.

Update alert trigger

Add the names of the administrators that want to be notified when ANR1073E, ANR1074E alerts occur, and also delete the name of an administrator that no longer wants to be notified, by issuing the following command:

```
update alerttrigger ANR1073E,ANR1074E ADDadmin=djee,cdawson,mhaye deladmin=harryh
```

Related commands

Table 1. Commands related to UPDATE ALERTTRIGGER

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.

Command	Description
UPDATE ALERTSTATUS (Update the status of an alert)	Updates the status of a reported alert.

UPDATE ALERTSTATUS (Update the status of an alert)

Use this command to update the status of a reported alert.

Privilege class

Any administrator can issue this command.

Syntax

```
                      .-,-----------.
                      V             |
>>-UPDate ALERTSTatus----+--alert_id-+--------------------------->

>--+------------------------+--+------------------+----------->
   '-STatus--=--+-Inactive-+-'  '-ASSigned--=--text-'
                '-Closed---'

>--+---------------------+--+----------------+---------------><
   '-RESolvedby--=--text-'  '-REMark--=--text-'
```

Parameters

alert_id (Required)
: Species the alert that you want to update. You can specify multiple message numbers by separating them with commas and no intervening spaces.

STatus
: Specifies the status type that you want to update. Alerts can be changed from active to inactive or closed, or from inactive to closed. Possible values are:

  Inactive
  : Active alerts can be changed to inactive status.

  Closed
  : Active and inactive alerts can be changed to closed status.

ASSigned
: Specifies the administrator name that is assigned the alert that you want to query.

RESolvedby
: Specifies the administrator name that resolved the alert that you want to query.

REMark
: This parameter specifies comment text. The comment text cannot exceed 255 characters. If the description contains any blank spaces, enclose the entire text in quotation marks (""). Remove previously defined text by specifying a null string ("") for this value.

Update the comment text in an alert

Issue the following command to update the comment text for alert ID number 25 and indicate that *DJADMIN* is working on the alert:

```
update alertstatus 25 assigned=DJADMIN
```

Update alert status

Issue the following command to change alert ID number 72 to the closed status, and add a remark about how the alert was resolved:

```
update alertstatus 72 status=closed remark="Increased the file system size for
 the active log"
```

Related commands

Table 1. Commands related to UPDATE ALERTSTATUS

Command	Description
DEFINE ALERTTRIGGER (Define an alert trigger)	Associates specified messages to an alert trigger.
DELETE ALERTTRIGGER (Remove a message from an alert trigger)	Removes a message number that can trigger an alert.
QUERY ALERTSTATUS (Query the status of an alert)	Displays information about alerts that have been issued on the server.
QUERY ALERTTRIGGER (Query the list of defined alert triggers)	Displays message numbers that trigger an alert.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
UPDATE ALERTTRIGGER (Update a defined alert trigger)	Updates the attributes of one or more alert triggers.

UPDATE ADMIN (Update an administrator)

Use this command to change the password or contact information for an administrator. However, you cannot update the SERVER_CONSOLE administrator name.

AIX Linux Passwords for administrators must be changed after a length of time that is determined by the SET PASSEXP command. The SET PASSEXP command does not affect passwords that authenticate with a Lightweight Directory Access Protocol (LDAP) server.

Restriction: You cannot update the authentication method for your own user ID. If necessary, another administrator must make that change. Also, when you update a password with the UPDATE ADMIN command, you cannot use a wildcard with the `admin_name` parameter.

Administrators with the same name as a node can be created during a REGISTER NODE command. To keep the node and administrator with the same name synchronized, the authentication method and the SSLREQUIRED setting for the node are updated to match the administrator. If the administrator authentication method is changed from LOCAL to LDAP and a password is not provided, the node is put in "LDAP pending" status. A password is then requested at the next logon. Passwords between same-named nodes and administrators are kept in sync through any authentication change.

You must use the RENAME ADMIN command to change the name of a registered administrator.

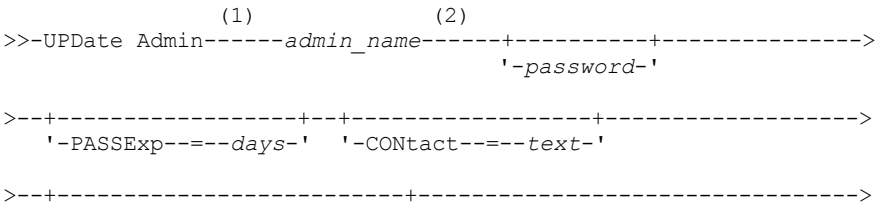
For users of Lightweight Directory Access Protocol (LDAP) servers:

- The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
- If an administrative user ID matches a node name, do not update the authentication method to LDAP. If you do, you might see unexpected behavior because of automatic password changes that update the same password twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update operation might fail.

Privilege class

To issue this command to change another administrator password or contact information, you must have system privilege. Any administrator can issue this command to update his or her own password or contact information.

Syntax



Notes:

1. You must specify at least one optional parameter on this command.
2. Passwords are optional for this command, except when changing the authentication method from LDAP to LOCAL.
3. The SYNCldapdelete parameter applies only if an administrator authenticating to an LDAP directory server reverts to local authentication.
4. The SSLREQUIRED parameter is deprecated.

Parameters

admin_name (Required)
: Specifies the name of the administrator to be updated.

password
: Specifies the administrator's password. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters. This parameter is optional in most cases. If the administrator authentication method is changed from LDAP to LOCAL, a password is required. If an LDAP server is used to authenticate administrators, do not specify a password by using the UPDATE ADMIN command.

PASSExp
: Specifies the number of days the password remains valid. You can set the password expiration period in the range 0 - 9999. A value of 0 means that the password never expires. This parameter is optional. If you do not specify this parameter, the password expiration period is unchanged. This parameter does not apply to passwords that are stored on an LDAP directory server.

CONtact
: Specifies a text string that identifies the administrator. This parameter is optional. Enclose the text string in quotation marks if it contains any blanks. To remove previously defined contact information, specify a null string ("").

FORCEPwreset
: Specifies whether the administrator is required to change or reset the password. This parameter is optional. Possible values are:

  No
  : Specifies that the administrator does not need to change or reset the password while attempting to sign on to the server. The password expiration period is set by the SET PASSEXP command.

  Yes
  : Specifies that the administrator's password will expire at the next sign-on. The administrator must change or reset the password then. If a password is not specified, you receive a syntax error.
  Restrictions:

- For administrative user IDs that authenticate with an LDAP server, password expiration is set by using LDAP server utilities. For this reason, do not specify FORCEPWRESET=YES if you plan to specify AUTHENTICATION=LDAP.
- If you plan to update an administrative user ID to authenticate with an LDAP server, and you specified FORCEPWRESET=YES, you must change the password before you can specify FORCEPWRESET=NO and AUTHENTICATION=LDAP.

EMAILADdress
: This parameter is used for additional contact information. The information that is specified by this parameter is not acted upon by IBM Spectrum Protect.

AUTHentication
: This parameter determines the password authentication method that the administrator ID uses; either LDAP or LOCAL.

  LOcal
  : Specifies that the administrator uses the local IBM Spectrum Protect server database to store passwords for authentication.

  LDap
  : Specifies that the administrator uses an LDAP directory server for password authentication.

SYNCldapdelete
: This parameter applies only if an administrator who authenticates to an LDAP server wants to revert to local authentication.

  Yes
  : Specifies that the administrator is deleted from the LDAP server.
  Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

  No
  : Specifies that the administrator is not deleted from the LDAP server. This is the default.

SSLrequired (deprecated)

: Specifies whether the administrator user ID must use the Secure Sockets Layer (SSL) protocol to communicate between the IBM Spectrum Protect server and the backup-archive client. When you authenticate passwords with an LDAP directory server, you must protect the sessions by using SSL or another network security method.

  Important: Beginning with IBM Spectrum Protect Version 8.1.2 software and Tivoli® Storage Manager Version 7.1.8 software, this parameter is deprecated. Validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The SSLREQUIRED parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

SESSIONSECurity
: Specifies whether the administrator must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

  You can specify one of the following values:

  STRict
  : Specifies that the strictest security settings are enforced for the administrator. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the server and the administrator. To specify whether the server uses TLS 1.2 for the entire session or only for authentication, see the SSL client option.
    To use the STRICT value, the following requirements must be met to ensure that the administrator can authenticate with the server:

    - Both the administrator and server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
    - The administrator must be configured to use the TLS 1.2 protocol for SSL sessions between the server and the administrator.

    Administrators set to STRICT that do not meet these requirements are unable to authenticate with the server.

  TRANSitional
  : Specifies that the existing security settings are enforced for the administrator. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the administrator has never met the requirements for the STRICT value, the administrator will continue to authenticate by using the TRANSITIONAL value. However, after an administrator meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the administrator can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after an administrator successfully authenticates by using a more secure communication protocol, the administrator can no longer authenticate by using a less secure protocol. For example, if an administrator that is not using SSL is updated and successfully authenticates by using TLS 1.2, the administrator can no longer authenticate by using no SSL protocol or TLS 1.1. This restriction also applies when you use functions such as command routing or server-to-server export, when the administrator authenticates to the IBM Spectrum Protect server as an administrator from another server.

ALert

Specifies whether alerts are sent to an administrators email address.

Yes

Specifies that alerts are sent to the specified administrators email address.

No

Specifies that alerts are not sent to the specified administrators email address. This is the default value.

Tip: Alert monitoring must be enabled, and email settings must be correctly defined to successfully receive alerts by email. To view the current settings, issue the QUERY MONITORSETTINGS command.

Example: Update a password and password expiration period

Update the administrator LARRY to have the password SECRETWORD and a password expiration period of 120 days. The administrator in this example is authenticated to the IBM Spectrum Protect server.

```
update admin larry secretword passexp=120
```

Example: Update all administrators to communicate with a server by using strict session security

Update all administrators to use the strictest security settings to authenticate with the server.

```
update admin * sessionsecurity=strict
```

Related commands

Table 1. Commands related to UPDATE ADMIN

Command	Description
QUERY ADMIN	Displays information about one or more IBM Spectrum Protect administrators.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
REGISTER NODE	Defines a client node to the server and sets options for that user.
RENAME ADMIN	Changes an IBM Spectrum Protect administrator's name.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
UPDATE NODE	Changes the attributes that are associated with a client node.

Related tasks:
Naming Tivoli Storage Manager objects
Related reference:
Ssl client option

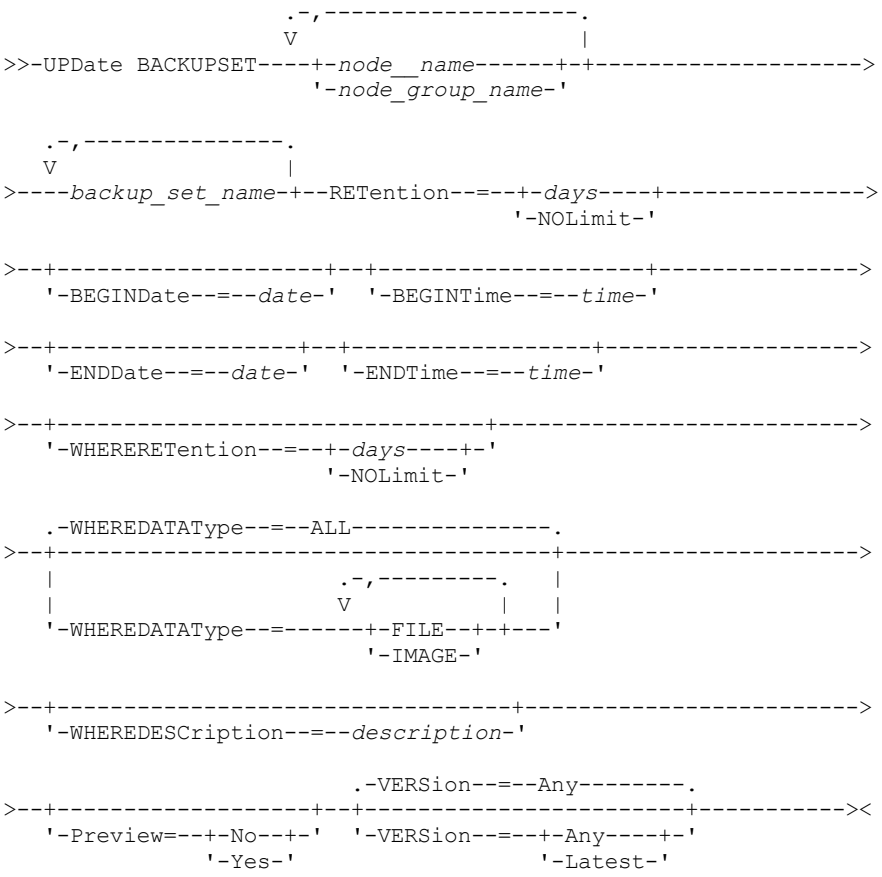
UPDATE BACKUPSET (Update a retention value assigned to a backup set)

Use this command to update the retention value associated with a client's backup set.

Privilege class

To issue this command, you must have system privilege or policy privilege for the domain to which the client node is assigned.

Syntax



Parameters

node_name or node_group_name (Required)
: Specifies the names of the client nodes or node groups whose data is contained in the specified backup set to be updated. To specify multiple node and node group names, separate the names with commas and no intervening spaces. The node names that you specify can contain wildcard characters, but node group names cannot contain wildcard characters.

backup_set_name (Required)
: Specifies the name of the backup set to update. The backup set name you specify can contain wildcard characters. You can specify more than one backup set name by separating the names with commas and no intervening spaces.

RETention (Required)
: Specifies the updated number of days to retain the backup set on the server. You can specify an integer from 0 to 30000. The values are:

  days
  : Specifies the updated number of days to retain the backup set.

  NOLimit
  : Specifies that the backup set is retained on the server indefinitely. If you specify NOLIMIT, the server retains the volumes containing the backup set forever, unless a user or administrator deletes the volumes from server storage. Attention: Updating the retention period of a backup set may cause it to expire at a different time from other backup sets that might be stored on the same output media. In either case, the media will not be made available for other

uses until all of its backup sets have expired.

BEGINDate

Specifies the beginning date in which the backup set to update was created. This parameter is optional. The default is the current date. You can use this parameter with the BEGINTIME parameter to specify a range for the date and time. If you specify a begin date without a begin time, the time will be at 12:00 a.m. (midnight) on the date you specify.
You can specify the date by using one of the following values:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified.	TODAY +3 *or* +3.
TODAY-days **or** -days	The current date minus days specified.	TODAY-3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

BEGINTime

Specifies the beginning time in which the backup set to update was created. This parameter is optional. The default is the current time. You can use this parameter with the BEGINDATE parameter to specify a range for the date and time. If you specify a begin time without a begin date, the date will be the current date at the time you specify.
You can specify the time by using one of the following values:

Value	**Description**	**Example**
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes on the specified end date	NOW+02:00 *or* +02:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes on the specified end date	NOW-02:00 *or* –02:00.

ENDDate

Specifies the ending date in which the backup set to update was created. This parameter is optional. You can use this parameter with the ENDTIME parameter to specify a range for the date and time. If you specify an end date without an ending time, the time will be at 11:59:59 p.m. on the specified end date.
You can specify the date by using one of the following values:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1999
TODAY	The current date	TODAY
TODAY+days *or* +days	The current date plus days specified.	TODAY +3 *or* +3.
TODAY-days *or* — days	The current date minus days specified.	TODAY -3 *or* -3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM

Value	Description	Example
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

ENDTime

Specifies the ending time in which the backup set to update was created. This parameter is optional. You can use this parameter with the ENDDATE parameter to specify a range for the date and time. If you specify an end time without an end date, the date will be the current date at the time you specify.

You can specify the time by using one of the following values:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM *or* +HH:MM	The current time plus hours and minutes specified	NOW+02:00 *or* +02:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW-02:00 *or* –02:00.

WHERERETention

Specifies the retention value, specified in days, that is associated with the backup set to update. The values are:

days
: Specifies that the backup set that is retained this number of days is updated.

NOLimit
: Specifies that the backup set retained indefinitely is updated.

WHEREDESCription

Specifies the description that is associated with the backup set to update. This parameter is optional. You can specify wildcard characters for the description. Enclose the description in quotation marks if it contains any blank characters.

WHEREDATAType

Specifies the backup sets containing the specified types of data are to be updated. This parameter is optional. The default is that backup sets for all types of data (file level, image, and application) are to be updated. To specify multiple data types, separate each data type with a comma and no intervening spaces. Possible values are:

ALL
: Specifies that backup sets for all types of data (file level, image, and application) are to be updated. This is the default.

FILE
: Specifies that a file level backup set is to be updated. File level backup sets contain files and directories backup up by the backup-archive client.

IMAGE
: Specifies that an image backup set is to be updated. Image backup sets contain images created by the backup-archive client BACKUP IMAGE command.

Preview

Specifies whether to preview the list of backup sets to update, without actually updating the backup sets. This parameter is optional. The default is No. The values are:

No
: Specifies that the backup sets are updated.

Yes
: Specifies that the server displays the backup sets to update, without actually updating the backup sets.

VERSion
: Specifies the version of the backup set to update. Backup sets with the same prefix name are considered to be different versions of the same backup set. This parameter is optional. The default is to update any version that matches the criteria specified on the command. The values are:

  Any
  : Specifies that any version that matches the criteria specified on the command should be updated.

  Latest
  : Specifies that only the most recent version of the backup set should be updated. If other criteria specified on the command (for example, ENDDATE or WHERERETENTION) exclude the most recent version of the backup set, then no backup set will be updated.

Example: Update a retention period

Update the retention period where the description is Healthy Computers. The retention period is assigned to backup set PERS_DATA.3099 that contains data from client node JANE. Change the retention period to 70 days.

```
update backupset jane pers_data.3099
retention=70 wheredescription="healthy computers"
```

Related commands

Table 1. Commands related to UPDATE BACKUPSET

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Updates a retention value associated with a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
GENERATE BACKUPSETTOC	Generates a table of contents for a backup set.
QUERY BACKUPSET	Displays backup sets.
QUERY BACKUPSETCONTENTS	Displays contents contained in backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE NODEGROUP	Updates the description of a node group.

UPDATE CLIENTOPT (Update a client option sequence number)

Use this command to update the sequence number of a client option in a client option set.

Privilege class

To issue this command, you must have system privilege or unrestricted policy privilege.

Syntax

```
>>-UPDate CLIENTOpt--option_set_name--option_name--------------->

>--current_sequence_number--new_sequence_number---------------><
```

Parameters

option_set_name (Required)
Specifies the name of the option set.
option_name (Required)
Specifies a valid client option.
current_sequence_number (Required)
Specifies the current sequence number of the option.
new_sequence_number (Required)
Specifies the new sequence number of the option.

Example: Update a client option sequence number

To update the current client option sequence number issue the following command:

```
update clientopt eng dateformat 0 9
```

Related commands

Table 1. Commands related to UPDATE CLIENTOPT

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.
QUERY CLOPTSET	Displays information about a client option set.

UPDATE CLOPTSET (Update a client option set description)

Use this command to update the description for a client option set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node is assigned.

Syntax

```
>>-UPDate CLOptset--option_set_name-----------------------------><

>--DESCription--=--description-----------------------------------><
```

Parameters

option_set_name (Required)
Specifies the name of the option set.
DESCription (Required)
Specifies a description of the client option set. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains blank characters.

Example: Update a client option set description

Update the description for a client option set named ENG.

```
update cloptset eng description="unix"
```

Related commands

Table 1. Commands related to UPDATE CLOPTSET

Command	Description
COPY CLOPTSET	Copies a client option set.
DEFINE CLIENTOPT	Adds a client option to a client option set.
DEFINE CLOPTSET	Defines a client option set.
DELETE CLIENTOPT	Deletes a client option from a client option set.
DELETE CLOPTSET	Deletes a client option set.
QUERY CLOPTSET	Displays information about a client option set.
UPDATE CLIENTOPT	Updates the sequence number of a client option in a client option set.

UPDATE COLLOCGROUP (Update a collocation group)

Use this command to modify the description of a collocation group.

Privilege class

To issue this command, you must have system or unrestricted storage privilege.

Syntax

```
>>-UPDate COLLOCGroup--group_name------------------------------>

>--DESCription--=--description---------------------------------><
```

Parameters

group_name
: Specifies the name of the collocation group whose description you want to update.

DESCription (Required)
: Specifies a description of the collocation group. This parameter is required. The maximum length of the description is 255 characters. If the description contains any blanks, enclose the entire description in quotation marks.

Example: Update a collocation group

Update the collocation group, GROUP1, with a new description.

```
update collocgroup group1 "Human Resources"
```

Related commands

Table 1. Commands related to UPDATE COLLOCGROUP

Command	Description
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
MOVE NODEDATA	Moves data for one or more nodes, or a single node with selected file spaces.
QUERY COLLOCGROUP	Displays information about collocation groups.

Command	Description
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY STGPOOL	Displays information about storage pools.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE STGPOOL	Changes the attributes of a storage pool.

UPDATE COPYGROUP (Update a copy group)

Use this command to update a backup or archive copy group. To allow clients to use the updated copy group, you must activate the policy set that contains the copy group.

Tip: The UPDATE COPYGROUP command fails if you specify a copy storage pool as a destination.

The UPDATE COPYGROUP command takes two forms, depending upon whether the update is for a backup copy group or for an archive copy group. The syntax and parameters for each form are defined separately.

Table 1. Commands related to UPDATE COPYGROUP

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
ASSIGN DEFMGMTCLASS	Assigns a management class as the default for a specified policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE MGMTCLASS	Defines a management class.
DELETE COPYGROUP	Deletes a backup or archive copy group from a policy domain and policy set.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
EXPIRE INVENTORY	Manually starts inventory expiration processing.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.

- UPDATE COPYGROUP (Update a backup copy group)
  Use this command to update a defined backup copy group.
- UPDATE COPYGROUP (Update a defined archive copy group)
  Use this command to update a defined archive copy group.

UPDATE COPYGROUP (Update a backup copy group)

Use this command to update a defined backup copy group.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the copy group belongs.

Syntax

```
>>-UPDate COpygroup--domain_name--policy_set_name--class_name--->

>--+----------+--+-----------------+--------------------------->
   '-STANDARD-'  '-Type--=--Backup-'

>--+---------------------------+--+--------------------+-------->
   '-DESTination--=--pool_name-'  '-FREQuency--=--days-'

>--+---------------------------+------------------------------->
   '-VERExists--=--+-number--+-'
                   '-NOLimit-'

>--+---------------------------+------------------------------->
   '-VERDeleted--=--+-number--+-'
                    '-NOLimit-'

>--+--------------------------+--+-------------------------+---->
   '-RETExtra--=--+-days----+-'  '-RETOnly--=--+-days----+-'
                  '-NOLimit-'                  '-NOLimit-'

>--+----------------------+---------------------------------->
   '-MODE--=--+-MODified-+-'
              '-ABSolute-'

>--+---------------------------------+------------------------>
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'

>--+---------------------------------+------------------------><
   '-TOCDestination--=----pool_name---'
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the copy group belongs.

policy_set_name (Required)
: Specifies the policy set to which the copy group belongs. You cannot update a copy group in the ACTIVE policy set.

class_name (Required)
: Specifies the management class to which the copy group belongs.

STANDARD
: Specifies the copy group, which must be STANDARD. This parameter is optional.

Type=Backup
: Specifies that you want to update a backup copy group. This parameter is optional.

DESTination
: Specifies the primary storage pool where the server initially stores backup data. This parameter is optional. You cannot specify a copy storage pool as the destination.

FREQuency
: Specifies how frequently the server can back up a file. This parameter is optional. The server backs up a file only when the specified number of days has elapsed since the last backup. The FREQUENCY value is used only during a full incremental backup operation. This value is ignored during selective backup or partial incremental backup. You can specify an integer from 0 to 9999. The value 0 means that the server can back up a file regardless of when the file was last backed up.

VERExists
: Specifies the maximum number of backup versions to retain for files that are currently on the client file system. This parameter is optional.
  If an incremental backup causes the limit to be exceeded, the server expires the oldest backup version that exists in server storage. Possible values are:

  number
  : Specifies the number of backup versions to retain for files that are currently on the client file system. You can specify an integer from 1 to 9999.
    Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 2. Preferred values are 3, 4, or more.

  NOLimit
  : Specifies that you want the server to retain all backup versions.

The number of backup versions to retain is controlled by this parameter until versions exceed the retention time specified by the RETEXTRA parameter.

VERDeleted
Specifies the maximum number of backup versions to retain for files that have been deleted from the client file system after being backed up using the server. This parameter is optional.
If a user deletes a file from the client file system, the next incremental backup causes the server to change the active backup version of the file to inactive and expire the oldest versions in excess of this number. The expiration date for the remaining versions is determined by the retention time specified by the RETEXTRA or RETONLY parameter. Possible values are:

number
Specifies the number of backup versions to retain for files that are deleted from the client file system after being backed up. You can specify a value from 0 to 9999.
NOLimit
Specifies that you want the server to retain all backup versions for files that are deleted from the client file system after being backed up.

RETExtra
Specifies the number of days that the server retains a backup version after that version becomes inactive. A version of a file becomes inactive when the client stores a more recent backup version, or when the client deletes the file from the workstation and then runs a full incremental backup. The server deletes inactive versions based on retention time even if the number of inactive versions does not exceed the number allowed by the VEREXISTS or VERDELETED parameters. This parameter is optional. Possible values are:

days
Specifies the number of days to retain inactive backup versions. You can specify an integer from 0 to 9999.
Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 14 days. The preferred value is 30 or more days.
NOLimit
Specifies that you want to retain inactive backup versions indefinitely.

If you specify NOLIMIT, the server deletes extra backup versions based on the VEREXISTS parameter (when the file still exists on the client file system) or the VERDELETED parameter (when the file no longer exists on the client file system).

RETOnly
Specifies the number of days to retain the last backup version of a file that has been deleted from the client file system. This parameter is optional. Possible values are:

days
Specifies the number of days to retain the last remaining inactive copy of a file. You can specify an integer from 0 to 9999.
Tip: To help ensure that files can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 30 days.
NOLimit
Specifies that you want to keep the last remaining inactive version of a file indefinitely.

If you specify NOLIMIT, the server retains the last remaining backup version forever, unless a user or administrator deletes the file from server storage.

MODE
Specifies whether the server backs up a file only if the file has changed since the last backup, or whenever a client requests a backup. This parameter is optional. Possible values are:

MODified
Specifies that the file is backed up only if it has changed since the last backup. A file is considered changed if any of the following is true:

- The date last modified is different
- The file size is different
- The file owner is different
- The file permissions are different

ABSolute

Specifies that the file is backed up regardless of whether it has been changed.

The MODE value is used only for full incremental backup. This value is ignored during partial incremental backup or selective backup.

SERialization

Specifies how the server processes files or directories when they are modified during backup processing. This parameter is optional. Possible values are:

SHRSTatic

Specifies that the server backs up a file or directory only if it is not being modified during backup. The server attempts to perform a backup as many as four times, depending on the value specified for the CHANGINGRETRIES client option. If the file or directory is modified during each backup attempt, the server does not back it up.

STatic

Specifies that the server backs up a file or directory only if it is not being modified during backup. The server attempts to perform the backup only once.

Platforms that do not support the STATIC option default to SHRSTATIC.

SHRDYnamic

Specifies that if the file or directory is being modified during a backup attempt, the server backs up the file or directory during the last attempt even though the file or directory is being modified. the server attempts to perform a backup as many as four times, depending on the value specified for the CHANGINGRETRIES client option.

DYnamic

Specifies that the server backs up a file or directory on the first attempt, regardless of whether the file or directory is being modified during backup processing.

Important: Be careful about using the SHRDYNAMIC and DYNAMIC values. IBM Spectrum Protect™ uses these values to determine if it backs up a file or directory while modifications are occurring. As a result, the backup version might be a fuzzy backup. A fuzzy backup does not accurately reflect what is currently in the file or directory because it contains some, but not all, modifications. If a file that contains a fuzzy backup is restored, the file may or may not be usable, depending on the application that uses the file. If a fuzzy backup is not acceptable, set SERIALIZATION to SHRSTATIC or STATIC so that IBM Spectrum Protect creates a backup version only if the file or directory is not being modified.

TOCDestination

Specifies the primary storage pool in which a table of contents (TOC) will initially be stored for any NDMP backup or backup set operation for which a TOC is generated. This parameter is optional. You cannot specify a copy storage pool as the destination. The storage pool specified for the destination must have NATIVE or NONBLOCK data format. To avoid mount delays, ensure that the storage pool has a device class of DISK or DEVTYPE=FILE. TOC generation is an option for NDMP backup operations, but is not supported for other image-backup operations.

To remove an existing TOC destination from the copy group, specify a null string ("") for this value.

If TOC creation is requested for a backup operation that uses NDMP and the image is bound to a management class whose backup copy group does not specify a TOC destination, the outcome will depend on the TOC parameter for the backup operation.

- If TOC=PREFERRED (the default), the backup proceeds without creation of a TOC.
- If TOC=YES, the entire backup fails because no TOC can be created.

Example: Update a backup copy group

Update the backup copy group (STANDARD) in the EMPLOYEE_RECORDS policy domain, VACATION policy set, ACTIVEFILES management class. Change the destination to DISKPOOL, with a minimum interval of seven days between backups, regardless of whether the files have been modified. Retain up to three backup versions while a file still exists on a client file system.

```
update copygroup employee_records vacation
activefiles type=backup destination=diskpool
frequency=7 verexists=3 mode=absolute
```

UPDATE COPYGROUP (Update a defined archive copy group)

Use this command to update a defined archive copy group.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the copy group belongs.

Syntax

```
>>-UPDate COpygroup--domain_name--policy_set_name--class_name--->

>--+----------+--Type--=--Archive------------------------------>
   '-STANDARD-'

>--+--------------------------+--+------------------+--------->
   '-DESTination--=--pool_name-'  '-FREQuency--=--Cmd-'

>--+------------------------+--+------------------+------------>
   '-RETVer--=--+-days----+-'  '-MODE--=--ABSolute-'
                '-NOLimit-'

>--+--------------------+-------------------------------------->
   '-RETMin--=----days---'

>--+---------------------------------+------------------------><
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the copy group belongs.

policy_set_name (Required)
: Specifies the policy set to which the copy group belongs. You cannot update a copy group in the ACTIVE policy set.

class_name (Required)
: Specifies the management class to which the copy group belongs.

STANDARD
: Specifies the copy group, which must be STANDARD. This parameter is optional.

Type=Archive (Required)
: Specifies that you want to update an archive copy group. This parameter is required.

DESTination
: Specifies the primary storage pool where the server initially stores the archive copy. This parameter is optional. You cannot specify a copy storage pool as the destination.

FREQuency=Cmd
: Specifies the copy frequency, which must be CMD. This parameter is optional.

RETVer
: Specifies the number of days to keep an archive copy. This parameter is optional. Possible values are:

  days
  : Specifies the number of days to keep an archive copy. You can specify an integer from 0 to 30000.
    Tip: To help ensure that your data can be recovered after a malware incident, such as a ransomware attack, specify a value of at least 30 days.

  NOLimit
  : Specifies that you want to keep an archive copy indefinitely.

    If you specify NOLIMIT, the server retains archive copies forever, unless a user or administrator deletes the file from server storage.

  The value of the RETVER parameter can affect the management class to which the server binds an archived directory. If the client does not use the ARCHMC option, the server binds directories that are archived to the default management class. If the default management class has no archive copy group, the server binds directories that are archived to the management class with the shortest retention period.

MODE=ABSolute
: Specifies that a file is always archived when the client requests it. The MODE must be ABSOLUTE. This parameter is optional.

RETMin
: Specifies the minimum number of days to keep an archive copy after it has been archived. This parameter is optional. The default value is 365.

SERialization
: Specifies how the server processes files that are modified during archive. This parameter is optional. Possible values are:

  SHRSTatic
  : Specifies that the server does not archive a file that is being modified. The server attempts to perform an archive as many as four times, depending on the value specified for the CHANGINGRETRIES client option. If the file is modified during the archive attempt, the server does not archive the file.

  STatic
  : Specifies that the server does not archive a file that is being modified. If a file is modified during the archive attempt, the server does not archive the file.

    Platforms that do not support the STATIC option default to SHRSTATIC.

  SHRDYnamic
  : Specifies that if the file is being modified during an archive attempt, the server archives the file during its last attempt even though the file is being modified. The server attempts to archive the file as many as four times, depending on the value specified for the CHANGINGRETRIES client option.

  DYnamic
  : Specifies that the server archives a file on the first attempt, regardless of whether the file is being modified during archive processing.

  Important: Be careful about using the SHRDYNAMIC and DYNAMIC values. IBM Spectrum Protect™ uses them to determine if it archives a file while modifications are occurring. As a result, the archive copy might be a fuzzy backup. A fuzzy backup does not accurately reflect what is currently in the file because it contains some, but not all, modifications. If a file that contains a fuzzy backup is retrieved, the file may or may not be usable, depending on the application that uses the file. If a fuzzy backup is not acceptable, set SERIALIZATION to SHRSTATIC or STATIC so that IBM Spectrum Protect creates an archive copy only if the file is not being modified.
  Tip: Be cautious when selecting retention values for primary storage pools that are of type RECLAMATIONTYPE=SNAPLOCK. Volumes in these types of storage pools cannot be deleted until after their retention dates have passed.

Example: Update multiple elements of a copy group

Update the archive copy group (STANDARD) in the EMPLOYEE_RECORDS policy domain, VACATION policy set, ACTIVEFILES management class. Change the destination to TAPEPOOL. Keep archive copies for 190 days.

```
update copygroup employee_records vacation
activefiles standard type=archive
destination=tapepool retver=190
```

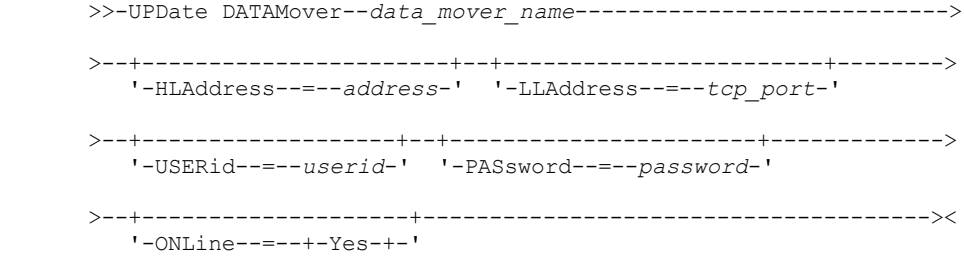
UPDATE DATAMOVER (Update a data mover)

Use this command to update the definition for a data mover or set a data mover off-line when the hardware is being maintained.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



```
'-No--'
```

Parameters

data_mover_name (Required)
: Specifies the name of the data mover.

HLAddress
: Specifies either the new numerical IP address or the new domain name, which is used to access the NAS file server. This parameter is optional.

LLAddress
: Specifies the new TCP port number to access the NAS file server for Network Data Management Protocol (NDMP) sessions. This parameter is optional.

USERid
: Specifies the user ID for a user that is authorized to initiate an NDMP session with the NAS file server. For example, enter the administrative ID for a NetApp file server. This parameter is optional.

PASsword
: Specifies the new password for the user ID to log onto the NAS file server. This parameter is optional.

ONLine
: Specifies whether the data mover is available for use. This parameter is optional.

  Yes
  : Specifies that the data mover is available for use.

  No
  : Specifies that the data mover is not available for use.
    Attention: If a library is controlled using a path from a data mover to the library, and the data mover is offline, the server will not be able to access the library. If the server is halted and restarted while the data mover is offline, the library will not be initialized.

Example: Update a data mover IP address

Update the data mover for the node named NAS1. Change the numerical IP address from 9.67.97.103 to 9.67.97.109.

```
update datamover nas1 hladdress=9.67.97.109
```

Example: Update a data mover domain name

Update the data mover for the node named NAS1. Change the numerical IP address from 9.67.97.109 to the domain name of NETAPP2.TUCSON.IBM.COM.

```
update datamover nas1 hladdress=netapp2.tucson.ibm.com
```

Related commands

Table 1. Commands related to UPDATE DATAMOVER

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DATAMOVER	Deletes a data mover.
QUERY DATAMOVER	Displays data mover definitions.
REGISTER NODE	Defines a client node to the server and sets options for that user.
UPDATE NODE	Changes the attributes that are associated with a client node.

UPDATE DEVCLASS (Update the attributes of a device class)

Use this command to update a defined device class.

Note: The DISK device class is predefined by IBM Spectrum Protect™ and cannot be modified with the UPDATE DEVCLASS command.

AIX Linux If you are updating a device class for devices that are to be accessed through a z/OS® media server, see UPDATE DEVCLASS - z/OS media server (Update device class for z/OS media server).

The syntax and parameter descriptions are provided according to the device type. The syntax and parameter information is presented in the following order.

- UPDATE DEVCLASS (Update a 3590 device class)
- UPDATE DEVCLASS (Update a 3592 device class)
- UPDATE DEVCLASS (Update a 4MM device class)
- UPDATE DEVCLASS (Update an 8MM device class)
- UPDATE DEVCLASS (Update a CENTERA device class)
- UPDATE DEVCLASS (Update a DLT device class)
- UPDATE DEVCLASS (Update an ECARTRIDGE device class)
- UPDATE DEVCLASS (Update a FILE device class)
- AIX Windows UPDATE DEVCLASS (Update a GENERICTAPE device class)
- UPDATE DEVCLASS (Update an LTO device class)
- UPDATE DEVCLASS (Update a NAS device class)
- UPDATE DEVCLASS (Update a REMOVABLEFILE device class)
- UPDATE DEVCLASS (Update a SERVER device class)
- UPDATE DEVCLASS (Update a VOLSAFE device class)

Table 1. Commands related to UPDATE DEVCLASS

Command	Description
BACKUP DEVCONFIG	Backs up IBM Spectrum Protect device information to a file.
DEFINE DEVCLASS	Defines a device class.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE DEVCLASS	Deletes a device class.
QUERY DEVCLASS	Displays information about device classes.
QUERY DIRSPACE	Displays information about FILE directories.
UPDATE LIBRARY	Changes the attributes of a library.

UPDATE DEVCLASS (Update a 3590 device class)

Use the 3590 device class when you are using 3590 tape devices.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see UPDATE DEVCLASS (Update a 3590 device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name--------------------------->

>--+-------------------------+--+----------------------+----->
   '-LIBRary---=--library_name-'  '-FORMAT---=--+-DRIVE---+-'
                                                +-3590B---+
                                                +-3590C---+
                                                +-3590E-B-+
                                                +-3590E-C-+
                                                +-3590H-B-+
                                                '-3590H-C-'

>--+---------------------+------------------------------------>
```

```
   '-ESTCAPacity--=--size-'

>--+-----------------------------------+-----------------------> 
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
Specifies the name of the device class to be defined.

LIBRary

Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

This parameter is optional.

For information about defining a library object, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following tables list the recording formats, estimated capacities, and recording format options for 3590 devices:

Table 1. Recording formats and default estimated capacities for 3590

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
3590B	10.0 GB	Uncompressed (basic) format
3590C	See note 20.0 GB	Compressed format
3590E-B	10.0 GB	Uncompressed (basic) format, similar to the 3590B format
3590E-C	See note 20.0 GB	Compressed format, similar to the 3590C format
3590H-B	30.0 GB (J cartridge-standard length) 60.0 GB (K cartridge-extended length)	Uncompressed (basic) format, similar to the 3590B format

Format	Estimated Capacity	Description
3590H-C	See note 60.0 GB (J cartridge-standard length) 120.0 GB (K cartridge-extended length)	Compressed format, similar to the 3590C format
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be greater than the listed value.		

Table 2. 3590 device recording format selections

Device	Format					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Read/Write	Read/Write	–	–	–	–
Ultra-SCSI	Read/Write	Read/Write	–	–	–	–
3590E	Read	Read	Read/Write	Read/Write	–	–
3590H	Read	Read	Read	Read	Read/Write	Read/Write

ESTCAPacity

Specifies the estimated capacity for the sequential access volumes that are categorized by this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

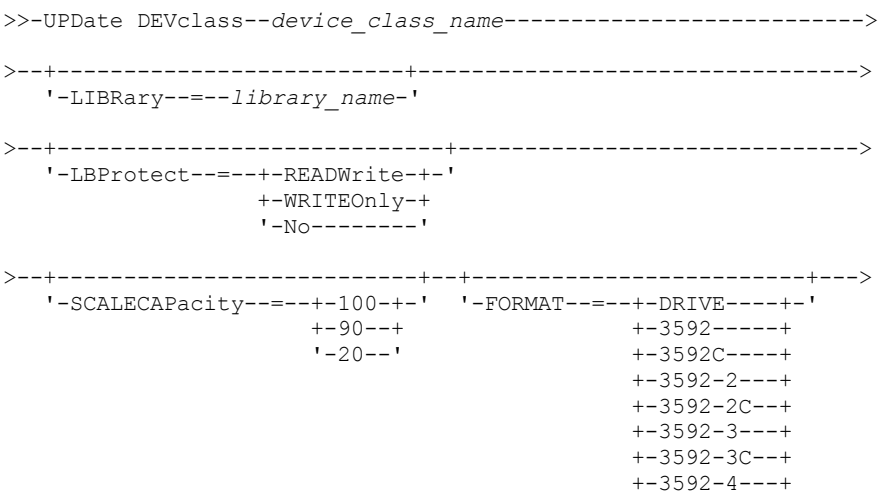
UPDATE DEVCLASS (Update a 3592 device class)

AIX | Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see UPDATE DEVCLASS (Update a 3592 device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



```
                                                +-3592-4C--+
                                                +-3592-5---+
                                                +-3592-5C--+
                                                +-3592-5A--+
                                                '-3592-5AC-'

>--+---------------------+-------------------------------------->
   '-ESTCAPacity--=--size-'

>--+-----------------------------------+----------------------->
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+--------------------------+------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'

>--+---------------------------------------------+------------><
   |  (1)   (2)                                  |
   '-------------DRIVEEncryption--=--+-ON-------+-'
                                     +-ALLOW----+
                                     +-EXTERNAL-+
                                     '-OFF------'
```

Notes:

1. You cannot specify both WORM=Yes and DRIVEENCRYPTION=ON.
2. Drive encryption is supported only for 3592 Generation 2 or later drives.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated. The maximum length of the device class name is 30 characters.

LIBRary

Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

This parameter is optional.

For information about defining a library object, see the DEFINE LIBRARY command.

LBProtect

Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

The following values are possible:

READWrite
Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect™ and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

WRITEOnly
Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to

generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

No
: Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

Restriction: Logical block protection is supported only on IBM® 3592 Generation 3 drives and later with 3592 Generation 2 media and later.

See Technote 1634851, Additional information on the Tivoli® Storage Manager LBProtect option, for an explanation about when to use the LBProtect parameter.

SCALECAPacity
: Specifies the percentage of the media capacity that can be used to store data. This parameter is optional. Possible values are 20, 90, or 100.

Setting the scale capacity percentage to 100 provides maximum storage capacity. Setting it to 20 provides fastest access time.

Note: The scale capacity value takes effect when data is first written to a volume. Any updates to the device class for scale capacity do not affect volumes that already have data that is written to them until the volume is returned to scratch status.

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats, estimated capacities, and recording format options for 3592 devices.
Tip: The format name is specified as, for example, 3592-X, 3592-XC, 3592-XA, or 3592-XAC, where X indicates the drive generation, C indicates a compressed format, and A indicates an archive drive.

Table 1. Recording formats and default estimated capacities for 3592

Format	Estimated capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
3592	300 GB	Uncompressed (basic) format
3592C	See note.	Compressed format
3592-2	500 GB 700 GB	Uncompressed (basic) format JA tapes Uncompressed (basic) format JB tapes
3592-2C	1.5 TB 2.1 TB	Compressed format JA tapes Compressed format JB tapes
3592–3	640 GB 1 TB	Uncompressed (basic) format JA tapes Uncompressed (basic) format JB tapes
3592–3C	1.9 TB 3 TB	Compressed format JA tapes Compressed format JB tapes

Format	Estimated capacity	Description
3592-4	400 GB	Uncompressed (basic) format JK tapes
	1.5 TB	Uncompressed (basic) format JB tapes
	3.1 TB	Uncompressed (basic) format JC tapes
3592-4C	1.2 TB	Compressed format JK tapes
	4.4 TB	Compressed format JB tapes
	9.4 TB	Compressed format JC tapes
3592-5 (For IBM TS1150 Model 3592 E08 drives with product ID 03592E08)	900 GB	Uncompressed (basic) format JK tapes
	7 TB	Uncompressed (basic) format JC/JY tapes
	2 TB	Uncompressed (basic) format JL tapes
	10 TB	Uncompressed (basic) format JD/JZ tapes
3592-5C (For IBM TS1150 Model 3592 E08 drives with product ID 03592E08)	Depends on the compressibility of the data	Compressed format JK tapes Compressed format JC/JY tapes Compressed format JL tapes Compressed format JD/JZ tapes
3592-5A (For IBM TS1155 Model 3592 55F drives with product ID 0359255F)	3 TB	Uncompressed (basic) format JL tapes
	15 TB	Uncompressed (basic) format JD/JZ tapes
3592-5AC (For IBM TS1155 Model 3592 55F drives with product ID 0359255F)	Depends on the compressibility of the data	Compressed format JL tapes Compressed format JD/JZ tapes
Note: If this format uses the compression feature for tape drives, depending on the effectiveness of compression, the actual capacity might be different from the estimated capacity.		

Important: For optimal performance, avoid mixing different generations of drives in a single SCSI library.

Special configurations are also required for mixing different generations of 3592 drives in 349x and ACSLS libraries.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

```
AB.CD2.E
```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

  However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption
: Specifies whether drive encryption is allowed. This parameter is optional.

  Updating this parameter affects empty volumes only. If a filling volume was previously encrypted or is unencrypted, and you update the DRIVEENCRYPTION parameter, the volume maintains its original encrypted or unencrypted status. The filling volume also maintains its original key-management status.

ON
: Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes-for example, back up sets, export volumes, and database backup volumes-will not be encrypted.) If you specify ON and you enable either the library or system method of encryption, drive encryption is not allowed and backup operations fail.

ALLOW
: Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if either the library or system method of encryption is enabled.

EXTERNAL
: Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive.
When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption.
By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF
: Specifies that drive encryption is not allowed. If you enable either the library or system method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

UPDATE DEVCLASS (Update a 4MM device class)

Use the 4MM device class when you are using 4 mm tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Parameters

device_class_name (Required)
Specifies the name of the device class to be defined.

LIBRary
Specifies the name of the defined library object that contains the 4 mm tape drives used by this device class. This parameter is optional. For information about defining a library object, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for 4 mm devices:

Table 1. Recording formats and default estimated capacities for 4 mm tapes

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
DDS1	1.3 GB (60 meter) 2.0 GB (90 meter)	Uncompressed format, applies only to 60-meter and 90-meter tapes
DDS1C	See note 1.3 GB (60 meter) 2.0 GB (90 meter)	Compressed format, applies only to 60-meter and 90-meter tapes
DDS2	4.0 GB	Uncompressed format, applies only to 120-meter tapes
DDS2C	See note 8.0 GB	Compressed format, applies only to 120-meter tapes
DDS3	12.0 GB	Uncompressed format, applies only to 125-meter tapes
DDS3C	See note 24.0 GB	Compressed format, applies only to 125-meter tapes
DDS4	20.0 GB	Uncompressed format, applies only to 150-meter tapes
DDS4C	See note 40.0 GB	Compressed format, applies only to 150-meter tapes
DDS5	36 GB	Uncompressed format, when using DAT 72 media
DDS5C	See note 72 GB	Compressed format, when using DAT 72 media
DDS6	80 GB	Uncompressed format, when using DAT 160 media
DDS6C	See note 160 GB	Compressed format, when using DAT 160 media

Format	Estimated Capacity	Description
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be greater than the listed value.		

ESTCAPacity

Specifies the estimated capacity for the sequential access volumes that are categorized by this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about the default estimated capacity for 4 mm tapes, see Table 1.

PREFIX

Specifies the high-level qualifier of the file name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
: Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
  Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
: Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
: Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

UPDATE DEVCLASS (Update an 8MM device class)

Use the 8MM device class when you are using 8 mm tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated.

LIBRary
Specifies the name of the defined library object that contains the 8 mm tape drives that can be used by this device class. For more information about defining a library object, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for 8 mm devices:

Table 1. Recording format and default estimated capacity for 8 mm tape

Format **Medium Type**	**Estimated Capacity**	**Description**
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
8200	2.3 GB	Uncompressed (standard) format, using standard 112-meter tape cartridges
8200C	See note 3.5 GB 4.6 GB	Compressed format, using standard 112-meter tape cartridges
8500 15m 15m 15m 54m 54m 54m 112m 112m 112m 160m XL	See note 600 MB 600 MB 600 MB 2.35 GB 2.35 GB 2.35 GB 5 GB or 10.0 GB 5 GB or 10.0 GB 5 GB or 10.0 GB 7 GB	Drives (Read Write) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW) Exabyte 8500/8500C (RW) Exabyte 8505 (RW) Eliant 820 (RW)

Format Medium Type	 Estimated Capacity	Description
8500C	See note	Drives (Read Write)
15m	1.2 GB	Eliant 820 (RW)
15m	1.2 GB	Exabyte 8500/8500C (RW)
15m	1.2 GB	Exabyte 8505 (RW)
54m	4.7 GB	Eliant 820 (RW)
54m	4.7 GB	Exabyte 8500/8500C (RW)
54m	4.7 GB	Exabyte 8505 (RW)
112m	5 GB or 10.0 GB	Eliant 820 (RW)
112m	5 GB or 10.0 GB	Exabyte 8500/8500C (RW)
112m	5 GB or 10.0 GB	Exabyte 8505 (RW)
160m XL	7 GB	Eliant 820 (RW)
8900	See note	Drive (Read Write)
15m	–	Mammoth 8900 (R)
54m	–	Mammoth 8900 (R)
112m	–	Mammoth 8900 (R)
160m XL	–	Mammoth 8900 (R)
22m	2.5 GB	Mammoth 8900 (RW)
125m	–	Mammoth 8900 (RW with upgrade)
170m	40 GB	Mammoth 8900 (RW)
AIT	See note	Drive
SDX1–25C	25 GB	AIT, AIT2 and AIT3 drives
SDX1–35C	35 GB	AIT, AIT2 and AIT3 drives
SDX2–36C	36 GB	AIT2 and AIT3 drives
SDX2–50C	50 GB	AIT2 and AIT3 drives
SDX3–100C	100 GB	AIT3, AIT4, and AIT5 drives
SDX3X-150C	150 GB	AIT3-Ex, AIT4, and AIT5 drives
SDX4–200C	200 GB	AIT4 and AIT5 drives
SDX5-400C	400 GB	AIT5 drive
AITC	See note	Drive
SDX1–25C	50 GB	AIT, AIT2 and AIT3 drives
SDX1–35C	91 GB	AIT, AIT2 and AIT3 drives
SDX2–36C	72 GB	AIT2 and AIT3 drives
SDX2–50C	130 GB	AIT2 and AIT3 drives
SDX3–100C	260 GB	AIT3, AIT4, and AIT5 drives
SDX3X-150C	390 GB	AIT3-Ex, AIT4, and AIT5 drives
SDX4–200C	520 GB	AIT4 and AIT5 drives
SDX5-400C	1040 GB	AIT5 drive
M2	See note	Drive (Read Write)
75m	20.0 GB	Mammoth II (RW)
150m	40.0 GB	Mammoth II (RW)
225m	60.0 GB	Mammoth II (RW)
M2C	See note	Drive (Read Write)
75m	50.0 GB	Mammoth II (RW)
150m	100.0 GB	Mammoth II (RW)
225m	150.0 GB	Mammoth II (RW)
SAIT	See note	Drive (Read Write)
	500 GB	Sony SAIT1–500(RW)
SAITC	See note	Drive (Read Write)
	1300 GB (1.3 TB)	Sony SAIT1–500(RW)

Format Medium Type	Estimated Capacity	Description
VXA2 V6 (62m) V10 (124m) V17 (170m)	See note 20 GB 40 GB 60 GB	Drive (Read Write) VXA–2
VXA2C V6 (62m) V10 (124m) V17 (170m)	See note 40 GB 80 GB 120 GB	Drive (Read Write) VXA–2
VXA3 X6 (62m) X10 (124m) X23 (230m)	See note 40 GB 86 GB 160 GB	Drive (Read Write) VXA–3
VXA3C X6 (62m) X10 (124m) X23 (230m)	See note 80 GB 172 GB 320 GB	Drive (Read Write) VXA–3
Note: The actual capacities might vary depending on which cartridges and drives are used. • For the AITC and SAITC formats, the normal compression ratio is 2.6:1. • For the M2C format, the normal compression ratio is 2.5:1.		

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about the default estimated capacity for 8 mm tapes, see Table 1.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

  However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

Example: Update the mount limit and capacity of an 8 mm device class

Update a device class named 8MMTAPE. Change the mount limit to 3 and the estimated capacity to 10 GB.

```
update devclass 8mmtape mountlimit=3 estcapacity=10G
```

Example: Update the mount retention period of an 8 mm device class

Update an 8 mm device class that is named 8MMTAPE to a 15-minute mount retention.

```
update devclass 8mmtape mountretention=15
```

UPDATE DEVCLASS (Update a CENTERA device class)

Use the CENTERA device class when you are using EMC Centera storage devices. The CENTERA device type uses files as volumes to store data sequentially. It is similar to the FILE device class.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name---------------------------->

                                    (1)
>--HLAddress--=--ip_address?PEA_file---------------------------->

>--+--------------------------+--------------------------------->
   '-MINCAPacity--=----size---'

>--+---------------------------+------------------------------><
   '-MOUNTLimit--=----number---'
```

Notes:

1. For each Centera device class, you must specify an IP address. However, a Pool Entry Authorization (PEA) file name and path are optional, and the PEA file specification must follow the IP address. Use the "?" character to separate the PEA file name and path from the IP address.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated. The maximum length of the device class name is 30 characters.

HLAddress
Specifies an IP address for the Centera storage device and, optionally, the name and path of one Pool Entry Authorization (PEA) file. Specify the IP address with the dotted decimal format (for example, 9.10.111.222). A Centera device might have multiple IP addresses. However, you must specify one of them as a value for this parameter.

AIX The PEA file name and path name are case-sensitive.

If you append the name and path of a PEA file, ensure that the file is stored in a directory on the system that runs the IBM Spectrum Protect™ server. Separate the PEA file name and path from the IP address or addresses with the "?" character, for example: Windows

```
HLADDRESS=9.10.111.222?c:\controlFiles\TSM.PEA
```

AIX

```
HLADDRESS=9.10.111.222?/user/ControlFiles/TSM.PEA
```

Specify only one PEA file name and path for each device class definition. If you specify two different Centera device classes that point to the same Centera storage device and if the device class definitions contain different PEA file names and paths, the server uses the PEA file that is specified in the device class HLADDRESS parameter that was first used to open the Centera storage device.
Note:

1. The server does not include a PEA file during installation. If you do not create a PEA file, the server uses the Centera default profile, which can allow applications to read, write, delete, purge, and query data on a Centera storage device. To provide tighter control, create a PEA file with the command-line interface that is provided by EMC Centera. For details about Centera authentication and authorization, refer to the EMC Centera *Programmer's Guide*.
2. You can also specify the PEA file name and path in an environment variable by using the syntax CENTERA_PEA_LOCATION=*filePath_ fileName*. The PEA file name and path that is specified with this environment variable apply to all Centera clusters. If you use this variable, you do not need to specify the PEA file name and path using the HLADDRESS parameter.
3. Updating the device class with a new or changed PEA file name and location might require a server restart if the Centera storage device identified by the IP address has already been accessed in the current instance of the server.

MINCAPacity
Specifies the new minimum size for Centera volumes that are assigned to a storage pool in this device class. This value represents the minimum amount of data that is stored on a Centera volume before the server marks it full. Centera volumes

continue to accept data until the minimum amount of data is stored. This parameter is optional.

size
Specify this value as an integer followed by K (kilobytes), M (megabytes), G (gigabytes), or T (terabytes). The minimum value that is allowed is 1 MB (MINCAPACITY=1M). The maximum value that is allowed is 128 GB (MINCAPacity=128G).

MOUNTLimit
Specifies the new maximum number of sessions that access the Centera device. This parameter is optional. You can specify any number from 0 or greater; however, the sum of all mount limit values for all device classes that are assigned to the same Centera device must not exceed the maximum number of sessions that are allowed by Centera.

UPDATE DEVCLASS (Update a DLT device class)

Use the DLT device class when you are using DLT tape devices.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated.

LIBRary
Specifies the name of the defined library object that contains the DLT tape drives that can be used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

The following table lists the recording formats and estimated capacities for DLT devices:

Table 1. Recording format and default estimated capacity for DLT

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
DLT1	40.0 GB	Uncompressed format, using only CompacTape III or CompacTape IV cartridges
DLT1C	See note 1. 80.0 GB	Compressed format, using only CompacTape III and CompacTape IV cartridges
DLT10	10.0 GB	Uncompressed format, using only CompacTape III or CompacTape IV cartridges
DLT10C	See note 1. 20.0 GB	Compressed format, using only CompacTape III and CompacTape IV cartridges
DLT15	15.0 GB	Uncompressed format, using only CompacTape IIIxt or CompacTape IV cartridges (not CompacTape III) Note: Valid with DLT2000XT, DLT4000, and DLT7000 drives
DLT15C	See note 1. 30.0 GB	Compressed format, using only CompacTape IIIxt or CompacTape IV cartridges (not CompacTape III) Valid with DLT2000XT, DLT4000, and DLT7000 drives
DLT20	20.0 GB	Uncompressed format, using only CompacTape IV cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT20C	See note 1. 40.0 GB	Compressed format, using only CompacTape IV cartridges Valid with DLT4000, DLT7000, and DLT8000 drives
DLT35	35.0 GB	Uncompressed format, using only CompacTape IV cartridges Valid with DLT7000 and DLT8000 drives
DLT35C	See note 1. 70.0 GB	Compressed format, using only CompacTape IV cartridges Valid with DLT7000 and DLT8000 drives

Format	Estimated Capacity	Description
DLT40	40.0 GB	Uncompressed format, using CompacTape IV cartridges Valid with a DLT8000 drive
DLT40C	See note 1. 80.0 GB	Compressed format, using CompacTape IV cartridges Valid with a DLT8000 drive
DLT2	80.0 GB	Uncompressed format, using Quantum DLT tape VS1 media
DLT2C	See note 1. 160.0 GB	Compressed format, using Quantum DLT tape VS1 media
DLT4	160.0 GB	Uncompressed format, using Quantum DLTtape VS1 cartridges. Valid with Quantum DLT-V4 drive
DLT4C	See note 1. 320.0 GB	Compressed format, using Quantum DLTtape VS1 cartridges. Valid with Quantum DLT-V4 drive
SDLT See note 2.	100.0 GB	Uncompressed format, using Super DLT Tape 1 cartridges Valid with a Super DLT drive
SDLTC See note 2.	See note 1. 200.0 GB	Compressed format, using Super DLT Tape 1 cartridges Valid with a Super DLT drive
SDLT320 See note 2.	160.0 GB	Uncompressed format, using Quantum SDLT I media Valid with a Super DLT drive
SDLT320C See note 2.	See note 1. 320.0 GB	Compressed format, using Quantum SDLT I media Valid with a Super DLT drive
SDLT600	300.0 GB	Uncompressed format, using SuperDLTtape-II media Valid with a Super DLT drive
SDLT600C	See note 1. 600.0 GB	Compressed format, using SuperDLTtape-II media Valid with a Super DLT drive
DLTS4	800 GB	Uncompressed format, using Quantum DLT S4 media. Valid with a DLT-S4 drive
DLTS4C	See note 1. 1.6 TB	Compressed format, using Quantum DLT S4 media. Valid with a DLT-S4 drive

Note:

1. Depending on the effectiveness of compression, the actual capacity might be greater than the listed value.
2. IBM Spectrum Protect™ does not support a library that contains both Backward Read Compatible (BRC) SDLT and Non-Backward Read Compatible (NBRC) SDLT drives.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about estimated capacities, see Table 1.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)

Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

UPDATE DEVCLASS (Update an ECARTRIDGE device class)

Use the ECARTRIDGE device class when you are using StorageTek drives such as the StorageTek T9840 or T10000.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see UPDATE DEVCLASS (Update an ECARTRIDGE device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name---------------------------->

>--+-------------------------+-------------------------------->
   '-LIBRary--=--library_name-'

>--+-----------------------------+------------------------------>
   '-LBProtect--=--+-READWrite-+-'
                   +-WRITEOnly-+
                   '-No--------'

>--+--------------------------+--+----------------------+------->
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--size-'
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

>--+-----------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+--------------------------+-------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'

>--+-----------------------------------------------+------------><
   |  (1)   (2)                                    |
   '-------------DRIVEEncryption--=--+-ON-------+-'
                                     +-ALLOW----+
                                     +-EXTERNAL-+
                                     '-OFF------'
```

Notes:

1. You can use drive encryption only for Oracle StorageTek T10000B drives with a format value of DRIVE, T10000B, or T10000B-C, for Oracle StorageTek T10000C drives with a format value of DRIVE, T10000C or T10000C-C, and for Oracle StorageTek T10000D drives with a format value of DRIVE, T10000D and T10000D-C.
2. You cannot specify both WORM=YES and DRIVEENCRYPTION=ON.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated.

LIBRary
Specifies the name of the defined library object with the ECARTRIDGE tape drives that can be used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

LBProtect

Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

The following values are possible:

READWrite
Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect™ and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

WRITEOnly
Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

No
Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

Restriction: Logical block protection is supported only on Oracle StorageTek T10000C and Oracle StorageTek T10000D drives.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

Important: If you specify DRIVE for a device class that has non-compatible sequential access devices, then you must mount volumes on devices that are capable of reading or writing the format that is established when the volume was first mounted. This can cause delays if the only sequential access device that can access the volume is already in use.
The following table lists the recording formats and estimated capacities for ECARTRIDGE devices:

Table 1. Recording formats and default estimated capacities for ECARTRIDGE tapes

Format	Estimated Capacity	Description

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

Notes:

- Some formats use a tape drive hardware compression feature. Depending on the effectiveness of compression, the actual capacity might be double or more than the listed value.
- T10000A drives can read and write the T10000A format only. T10000B drives can read, but cannot write, the T10000A format. T10000C drives can read, but cannot write, the T10000A and T10000B formats. T10000D drives can read, but cannot write, the T10000A, T10000B, and T10000C formats.

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about the default estimated capacity for cartridge tapes, see Table 1.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

  However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption
: Specifies whether drive encryption is allowed. This parameter is optional.
  Restriction:

  1. You can use drive encryption only for the following drives:
     - Oracle StorageTek T10000B drives that have a format value of DRIVE, T10000B, or T10000B-C
     - Oracle StorageTek T10000C drives that have a format value of DRIVE, T10000C, or T10000C-C
     - Oracle StorageTek T10000D drives that have a format value of DRIVE, T10000D, or T10000D-C

2. You cannot specify IBM Spectrum Protect as the key manager for drive encryption of WORM (write once, read many) media. (Specifying both WORM=YES and DRIVEENCRYPTION=ON is not supported.)
3. If encryption is enabled for a device class, and the device class is associated with a storage pool, the storage pool should not share a scratch pool with other device classes that cannot be encrypted. If a tape is encrypted, and you plan to use it on a drive that cannot be encrypted, you must manually relabel the tape before it can be used on that drive.

ON
: Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes are not encrypted. For example, back up sets, export volumes, and database backup volumes are not encrypted.) If you specify ON and you enable another method of encryption, drive encryption is not allowed and backup operations fail.

ALLOW
: Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if another method of encryption is enabled.

EXTERNAL
: Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive. When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption. By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF
: Specifies that drive encryption is not allowed. If you enable another method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

UPDATE DEVCLASS (Update a FILE device class)

Use the FILE device class when you are using files on magnetic disk storage as volumes that store data sequentially (as on tape).

AIX Linux The FILE device class does not support EXTERNAL libraries.

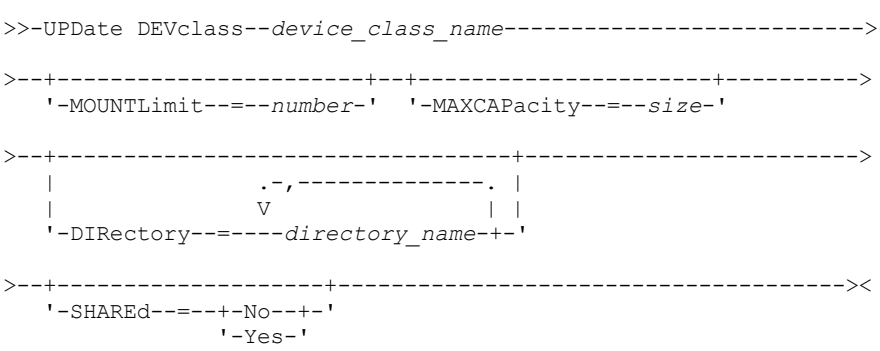
Windows The FILE device class does not support EXTERNAL libraries.

AIX Linux If you are defining a device class for devices that are to be accessed through a z/OS® media server, see UPDATE DEVCLASS (Update a FILE device class for z/OS media server).

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
: Specifies the name of the device class to be updated.

MOUNTLimit

Specifies the maximum number of files that can be simultaneously open for input and output. This parameter is optional. You can specify a number from 0 to 4096.

Windows If the device class is shared with a storage agent (by specifying the SHARED=YES parameter), drives are defined or deleted to match the MOUNTLIMIT value.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

MAXCAPacity
Specifies the maximum size of any data storage files that are categorized by this device class. This parameter is optional.

Specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The minimum size is 1 MB (MAXCAPACITY=1M). If you are defining a FILE device class for database-backup volumes, specify a value for MAXCAPACITY that is appropriate for the size of the database and that minimizes the number of database volumes.

For example, MAXCAPACITY=5G specifies that the maximum capacity for a volume in this device class is 5 gigabytes. The value that is specified must be less than or equal to the maximum supported size of a file on the target file system.

AIX Linux Do not define a MAXCAPACITY value greater than 640M when this file is for REMOVABLEFILE CD support. A value less than a CD's usable space (650 MB) allows for a one-to-one match between files from the FILE device class and copies that are on CD.

DIRectory
Specifies the directory location or locations of the files that are used in this device class. Enclose the entire list of directories within quotation marks, by using commas to separate individual directory names. Special characters (for example, blank spaces) are allowed within directory names. For example, the directory list "abc def,xyz" contains two directories: abc def and xyz. This parameter is optional.

By specifying a directory name or names, you identify the locations where the server places the files that represent storage volumes for this device class.

AIX Linux While the command is processed, the server expands the specified directory name or names into their fully qualified forms, starting from the root directory.

Important: If you are using storage agents for shared access to FILE volumes, you must use the DEFINE PATH command to define a path for each storage agent. The path definition includes the directory names that are used by the storage agent to access each directory.

Later, if the server must allocate a scratch volume, it creates a new file in one of these directories. (The server can choose any of the directories in which to create new scratch volumes.) For scratch volumes used to store client data, the file that is created by the server has a file name extension of .bfs. For scratch volumes used to store export data, a file name extension of .exp is used.

AIX Linux For example, if you define a device class with a directory of tsmstor and the server needs a scratch volume in this device class to store export data, the file that the server creates might be named /tsmstor/00566497.exp.

Windows For example, if you define a device class with a directory of c:\server and the server needs a scratch volume in this device class to store export data, the file that the server creates might be named c:\server\00566497.exp.

Tip: If you specify multiple directories for a device class, ensure that the directories are associated with separate file systems. Space trigger functions and storage pool space calculations take into account the space that remains in each directory. If you specify multiple directories for a device class and the directories are in the same file system, the server calculates space by adding values that represent the space that remains in each directory. These space calculations are inaccurate. Rather than choosing a storage pool with sufficient space for an operation, the server might choose the wrong storage pool and run out of space prematurely. For space triggers, an inaccurate calculation might result in a failure to expand the space available in a storage pool. Failure to expand space in a storage pool is one of the conditions that can cause a trigger to become disabled. If a trigger is disabled because the space in a storage pool was not expanded, you can re-enable the trigger by issuing the following command: `update spacetrigger stg`. No further changes are required to the space trigger.
Restriction: To modify a list of directories, you must replace the entire list.

SHAREd
Specifies that this FILE device class is shared between the server and one or more storage agents. To prepare for sharing, a library is automatically defined along with a number of drives corresponding to the MOUNTLIMIT associated with the

device class. If the library and drives exist and the MOUNTLIMIT is changed, drives can either be created to reach a new higher MOUNTLIMIT value or deleted to reach a new lower value.

Storage agents using FILE volumes

You must ensure that storage agents can access newly created FILE volumes. To access FILE volumes, storage agents replace names from the directory list in the device-class definition with the names in the directory list for the associated path definition. The following illustrates the importance of matching device classes and paths to ensure that storage agents can access newly created FILE volumes.

Suppose you want to use these three directories for a FILE library:

Windows

- c:\server
- d:\server
- e:\server

AIX

- /usr/tivoli1
- /usr/tivoli2
- /usr/tivoli3

Linux

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. You use the following command to set up a FILE library named CLASSA with one drive named CLASSA1 on SERVER1:

   Windows

   ```
   define devclass classa devtype=file
   directory="c:\server,d:\server,e:\server"
   shared=yes mountlimit=1
   ```

   AIX

   ```
   define devclass classa devtype=file
   directory="/usr/tivoli1,/usr/tivoli2,/usr/tivoli3"
   shared=yes mountlimit=1
   ```

   Linux

   ```
   define devclass classa devtype=file
   directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
   shared=yes mountlimit=1
   ```

2. You want the storage agent STA1 to be able to use the FILE library, so you define the following path for storage agent STA1:

   - Windows

     ```
     define path server1 sta1 srctype=server desttype=drive device=file
     directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
     \\192.168.1.10\e\server" library=classa
     ```

     In this scenario, the storage agent, STA1, replaces the directory name c:\server with the directory name \\192.168.1.10\c\server to access FILE volumes that are in the c:\server directory on the server.

   - AIX

     ```
     define path server1 sta1 srctype=server desttype=drive device=file
     directory="/usr/ibm1,/usr/ibm2,/usr/ibm3" library=classa
     ```

     In this scenario, the storage agent, STA1, replaces the directory name /usr/tivoli1 with the directory name /usr/ibm1 to access FILE volumes that are in the /usr/tivoli1 directory on the server.

   - Linux

```
define path server1 sta1 srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

In this scenario, the storage agent, STA1, replaces the directory name /opt/tivoli1 with the directory name /opt/ibm1/ to access FILE volumes that are in the /opt/tivoli1 directory on the server.

The following results occur:

- Windows File volume c:\server\file1.dsm is created by SERVER1. If you later change the first directory for the device class with the following command:

  ```
  update devclass classa directory="c:\otherdir,d:\server,e:\server"
  ```

  SERVER1 is still able to access file volume c:\server\file1.dsm, but the storage agent STA1 is not able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list that is associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume is still accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.
- AIX If file volume /usr/tivoli1/file1.dsm is created on SERVER1, and if the following command is issued,

  ```
  update devclass classa directory="/usr/otherdir,/usr/tivoli2,
  /usr/tivoli3"
  ```

  SERVER1 is still able to access file volume /usr/tivoli1/file1.dsm, but the storage agent STA1 is not able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list that is associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume is still accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.
- Linux If file volume /opt/tivoli1/file1.dsm is created on SERVER1, and if the following command is issued,

  ```
  update devclass classa directory="/opt/otherdir,/opt/tivoli2,
  /opt/tivoli3"
  ```

  SERVER1 is still able to access file volume /opt/tivoli1/file1.dsm, but the storage agent STA1 is not able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list that is associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume is still accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.

Example: Update a FILE device class for sharing

Prepare a FILE device class (named PLAINFILES) for sharing with an IBM Spectrum Protect™ storage agent.

```
update devclass plainfiles shared=yes
```

Example: Update the capacity of a FILE device class

Update a file device class named STORFILES to a maximum capacity of 25 MB.

```
update devclass storfiles maxcap=25m
```

AIX

Example: Add a directory to a FILE device class

Update the FILE device class, CLASSA, by adding a directory, /usr/otherdir, to the directory list. The directories /opt/tivoli2 and /opt/tivoli3 were specified when the device class was first defined.

```
update devclass classa
 directory="/opt/tivoli2,/opt/tivoli3,/usr/otherdir"
```

Linux

Example: Add a directory to a FILE device class

Update the FILE device class, CLASSA, by adding a directory, /usr/otherdir, to the directory list. The directories /usr/tivoli2 and /usr/tivoli3 were specified when the device class was first defined.

```
update devclass classa
directory="/usr/tivoli2,/usr/tivoli3,/usr/otherdir"
```

Windows

Example: Add a directory to a FILE device class

Update the FILE device class, CLASSA, by adding a directory, c:\otherdir, to the directory list. The directories d:\server and e:\server were specified when the device class was first defined.

```
update devclass classa
 directory="d:\server,e:\server,c:\otherdir"
```

AIX | Windows

UPDATE DEVCLASS (Update a GENERICTAPE device class)

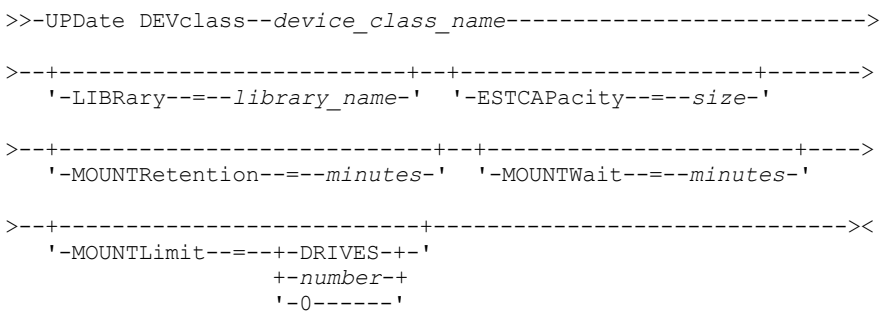
Use the GENERICTAPE device class for tape drives that are supported by operating system device drivers.

When this device type is used, the server does not recognize either the type of device or the cartridge recording format. Because the server does not recognize the type of device, if an I/O error occurs, error information is less detailed compared to error information for a specific device type (for example, 8MM). When you define devices to the server, do not mix various types of devices within the same device type.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

device_class_name (Required)
: Specifies the name of the device class to be updated.

LIBRary
: Specifies the name of the defined library object that contains the tape drives that can be used by this device class.

  This parameter is optional.

  For information about defining a library object, see the DEFINE LIBRARY command.

ESTCAPacity
: Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

  You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

  Specify a capacity appropriate to the particular tape drive that is being used.

  You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

MOUNTRetention
Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

UPDATE DEVCLASS (Update an LTO device class)

Use the LTO device class when you are using LTO tape devices.

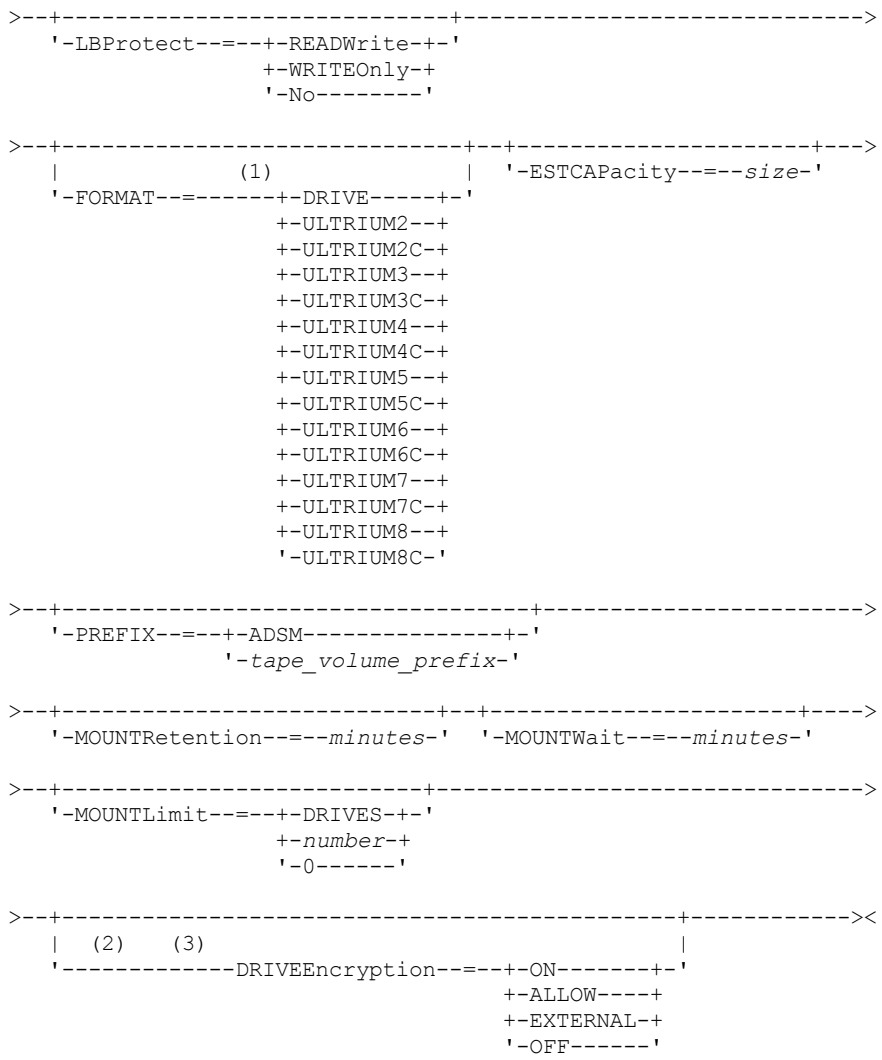
Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name--------------------------->

>--+-------------------------+--------------------------------->
   '-LIBRary--=--library_name-'
```



Notes:

1. IBM Spectrum Protect™ server supports LTO-2 tape drives; however, IBM® Tape Device drivers do not. In the event of an issue with the LTO-2 drive, the preferred corrective action is to upgrade your tape drive hardware to a higher generation drive, then install the latest version of the device driver.
2. You cannot specify DRIVEENCRYPTION=ON if your drives are using WORM (write once, read many) media.
3. Drive encryption is supported only for LTO-4 and higher generation LTO drives and media.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated. The maximum length of the device class name is 30 characters.

LIBRary
Specifies the name of the defined library object that contains the LTO tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

LBProtect

Specifies whether logical block protection is used to ensure the integrity of data stored on tape. When LBPROTECT is set to READWRITE or to WRITEONLY, the server uses this feature of the tape drive for logical block protection and generates cyclic redundancy check (CRC) protection information for each data block written on tape. The server also validates the CRC protection information when data is read from the tape.

The following values are possible:

READWrite

Specifies that logical block protection is enabled in the server and the tape drive for both read and write operations. Data is stored with CRC information in each block. This mode affects performance because additional processor usage is required for IBM Spectrum Protect and the tape drive to calculate and compare CRC values. The READWRITE value does not affect backup sets and data that is generated by the BACKUP DB command.

When the LBPROTECT parameter is set to READWRITE, you do not have to specify the CRCDATA parameter in a storage pool definition because logical block protection provides better protection against data corruption.

WRITEOnly
Specifies that logical block protection is enabled in the server and the tape drive for write operations only. Data is stored containing CRC information in each block. For read operations, the server and the tape drive do not validate the CRC. This mode affects performance because additional processor usage is required for IBM Spectrum Protect to generate the CRC and for the tape drive to calculate and compare CRC values for write operations. The WRITEONLY value does not affect backup sets and data that are generated by the BACKUP DB command.

No
Specifies that logical block protection is not enabled in the server and the tape drive for read and write operations. However, the server enables logical block protection on write operations for a filling volume that already has data with logical block protection.

Restriction:
Restrictions apply to logical block protection (LBP):

- At the LTO-5 level, LBP is supported only on IBM LTO-5.
- Starting with LTO-6, LBP is supported by all LTO drive vendors.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional.

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Instead, specify the format that the drives use.

- If you plan to upgrade all drives to Generation 4, 5, 6, 7, or 8, you must delete all existing LTO Ultrium drive definitions and the paths that are associated with them. Then, you can define the new Generation 4, 5, 6, 7, or 8 drives and paths.
- LTO-8 drives are unable to read LTO-6 media. If you are mixing LTO-6 with LTO-8 drives and media in a single library, you must partition the library into two libraries. One library must have only LTO-8 drives and media and the other must have LTO-6 drives and media.

If you are considering mixing different generations of LTO media and drives, be aware of the following restrictions.

Table 1. Read - write capabilities for different generations of LTO drives

Drives	Generation 3 media	Generation 4 media	Generation 5 media	Generation 6 media	Generation 7 media	Generation M8 media	Generation 8 media
Generation 3 [1]	Read and write	n/a	n/a	n/a	n/a	n/a	n/a
Generation 4 [1]	Read and write	Read and write	n/a	n/a	n/a	n/a	n/a
Generation 5 [1]	Read only	Read and write	Read and write	n/a	n/a	n/a	n/a
Generation 6 [1]	n/a	Read only	Read and write	Read and write	n/a	n/a	n/a
Generation 7 [1]			Read only	Read and write	Read and write	n/a	n/a
Generation 8 [2]	n/a	n/a	n/a	n/a	Read and write	Read and write	Read and write

Drives	Generation 3 media	Generation 4 media	Generation 5 media	Generation 6 media	Generation 7 media	Generation M8 media	Generation 8 media
[1] If a storage pool volume can only be read by a tape drive, ensure that the attributes of the storage pool volume are set to read only. [2] LTO-8 drives have two media types: LTO-M8 media and LTO-8 media. Both media types are used only in LTO-8 tape drives.							

The following table lists the recording formats and estimated capacities for LTO devices:

Table 2. Recording format and default estimated capacity for LTO

Format	Estimated capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
ULTRIUM2	200 GB	Uncompressed (standard) format, using Ultrium 2 cartridges
ULTRIUM2C	See note 400 GB	Compressed format, using Ultrium 2 cartridges
ULTRIUM3	400 GB	Uncompressed (standard) format, using Ultrium 3 cartridges
ULTRIUM3C	See note 800 GB	Compressed format, using Ultrium 3 cartridges
ULTRIUM4	800 GB	Uncompressed (standard) format, using Ultrium 4 cartridges
ULTRIUM4C	See note 1.6 TB	Compressed format, using Ultrium 4 cartridges
ULTRIUM5	1.5 TB	Uncompressed (standard) format, using Ultrium 5 cartridges
ULTRIUM5C	Varied, as described in note	Compressed format, using Ultrium 5 cartridges
ULTRIUM6	2.5 TB	Uncompressed (standard) format, using Ultrium 6 cartridges
ULTRIUM6C	Varied, as described in note	Compressed format, using Ultrium 6 cartridges
ULTRIUM7	6 TB	Uncompressed (standard) format, using Ultrium 7 cartridges
ULTRIUM7C	Varied, as described in note	Compressed format, using Ultrium 7 cartridges
ULTRIUM8	12 TB for LTO-8 media 9 TB for LTO-M8 media	Uncompressed (standard) format, using Ultrium M8 or Ultrium 8 cartridges
ULTRIUM8C	Varied, as described in note	Compressed format, using Ultrium M8 or Ultrium 8 cartridges
Note: If this format uses the tape-drive hardware-compression feature, depending on the effectiveness of compression, the actual capacity is varied.		

ESTCAPacity

Specifies the estimated capacity for the sequential access volumes that are categorized by this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about estimated capacities, see Table 2.

PREFIX

Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

MOUNTRetention

Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

However, for EXTERNAL library types, setting this parameter to a low value (for example, two minutes) enhances device sharing between applications.

Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait

Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit

Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

The following are possible values:

DRIVES

Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

number

Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

0 (zero)
Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

DRIVEEncryption
Specifies whether drive encryption is allowed. This parameter is optional. Drive encryption is supported only for LTO-4 and higher generation drives and media.
Restriction: If encryption is enabled for a device class, and the device class is associated with a storage pool, the storage pool should not share a scratch pool with other device classes that cannot be encrypted. If a tape is encrypted, and you plan to use it on a drive that cannot be encrypted, you must manually relabel the tape before it can be used on that drive.

ON
Specifies that IBM Spectrum Protect is the key manager for drive encryption and allows drive encryption for empty storage pool volumes only if the application method is enabled. (Other types of volumes are not encrypted. For example, back up sets, export volumes, and database backup volumes are not encrypted.) If you specify ON and you enable another method of encryption, drive encryption is not allowed and backup operations fail.
Note: You cannot specify IBM Spectrum Protect as the key manager for drive encryption of WORM (write once, read many) media. (If you are using WORM media, you cannot specify DRIVEENCRYPTION=ON.)

ALLOW
Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. However, drive encryption for empty volumes is allowed if another method of encryption is enabled.

EXTERNAL
Specifies that IBM Spectrum Protect does not manage the keys for drive encryption. Use this setting with an encryption methodology that is provided by another vendor and that is used with Application Method Encryption (AME) enabled on the drive. When you specify EXTERNAL and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect does not turn off encryption. By contrast, when you specify ALLOW and IBM Spectrum Protect detects that AME encryption is enabled, IBM Spectrum Protect turns off encryption.

OFF
Specifies that drive encryption is not allowed. If you enable another method of encryption, backups fail. If you enable the application method, IBM Spectrum Protect disables encryption and backups are attempted.

Example: Update the mount limit for an LTO device class

Update a device class named LTOTAPE. Change the mount limit to 2.

```
update devclass ltotape mountlimit=2
```

UPDATE DEVCLASS (Update a NAS device class)

Use the NAS device class when you are using NDMP (Network Data Management Protocol) operations to back up network-attached storage (NAS) file servers. The device class is for drives that are supported by the NAS file server for backups.

AIX | Linux The NAS device class does not support EXTERNAL libraries.

Windows The NAS device class does not support EXTERNAL libraries.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name--------------------------->

>--+-------------------------+--+----------------------+------->
   '-LIBRary--=--library_name-'  '-MOUNTRetention--=--0-'

>--+-----------------------+--+--------------------------+----->
   '-MOUNTWait--=--minutes-'  '-MOUNTLimit--=--+-DRIVES-+-'
                                               +-number-+
                                               '-0------'
```

```
>--+---------------------+-------------------------------------->
   '-ESTCAPacity--=--size-'

>--+-----------------------------+-------------------------><
   '-PREFIX--=--tape_volume_prefix-'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

LIBRary
: Specifies the name of the defined library object that contains the SCSI tape drives used by this device class. For information about defining a library object, see the DEFINE LIBRARY command.

MOUNTRetention=0
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. Zero (0) is the only supported value for device classes with DEVType=NAS.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

ESTCAPacity

: Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

  You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

  For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

  To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

PREFIX
: Specifies the high-level qualifier of the data set name that the server writes into the sequential access media labels. For each sequential access volume assigned to this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a tape volume data set name using the default prefix is ADSM.BFS.

Example: Update the estimated capacity for a NAS device class

Update a device class named NASTAPE. Change the estimated capacity to 200 GB.

```
update devclass nastape library=naslib estcapacity=200G
```

UPDATE DEVCLASS (Update a REMOVABLEFILE device class)

Use the REMOVABLEFILE device class for removable media devices that are attached as local, removable file systems.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name---------------------------->

>--+-------------------------+--+---------------------+------->
   '-LIBRary--=--library_name-'  '-MAXCAPacity--=--size-'

>--+---------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+-------------------------+-----------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be updated.

LIBRary
: Specifies the name of the defined library object that contains the removable media drives used by this device class. This parameter is optional. For information about defining a library object, see the DEFINE LIBRARY command.

MAXCAPacity
: Specifies the maximum size of any volumes that are defined to a storage pool categorized by this device class. This parameter is optional.

  AIX Windows Because the server opens only one file per physical removable medium, specify a capacity that enables one file to make full use of your media capacity.

  You must specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes).

  For example, MAXCAPACITY=5M specifies that the maximum capacity for a volume in this device class is 5 MB. The smallest value that is allowed is 1 MB (that is, MAXCAPACITY=1M).

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

UPDATE DEVCLASS (Update a SERVER device class)

Use the SERVER device class to use storage volumes or files that are archived in another IBM Spectrum Protect™ server.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDdate DEVclass--device_class_name-------------------------->

>--+-----------------------------+--+----------------------+----->
   '-SERVERName--=--server_name-'  '-MAXCAPacity--=--size-'

>--+-----------------------------------+------------------------>
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

>--+-----------------------------+----------------------------->
   '-RETRYPeriod--=----minutes---'
```

```
>--+------------------------------+--------------------------->
   '-RETRYInterval--=----seconds---'

>--+----------------------------+------------------------------>
   '-MOUNTRetention--=--minutes-'

>--+--------------------------+------------------------------><
   '-MOUNTLimit--=--+-number-+-'
                    '-1------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be updated.

SERVERName
: Specifies the name of the server. The SERVERNAME parameter must match a defined server.
Note: If you change the SERVERNAME of an existing server to a new name, data on the volumes under the old SERVERNAME is no longer accessible with this device class.

MAXCAPacity
: Specifies the maximum size that objects can be when created on the target server. This parameter is optional.

  Specify this value as an integer followed by `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The minimum value that is allowed is 1 MB (MAXCAPACITY=1M).

PREFIX
: Specifies the beginning portion of the high-level archive file name on the target server. This parameter is optional. The maximum length of this prefix is 8 characters.

  If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

  Values that are specified for this parameter must meet the following conditions:

  - The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

    ```
    AB.CD2.E
    ```

  - The qualifiers must be separated by a single period.
  - The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

  An example of a high-level archive file name that uses the default prefix is ADSM.volume1.

RETRYPeriod
: Specifies the retry period in minutes. The retry period is the interval during which the server attempts to contact a target server if there is a suspected communications failure. This parameter is optional. You can specify a number 0 - 9999.

RETRYInterval
: Specifies the retry interval in seconds. The retry interval is how often retries are done within a specific time period. This parameter is optional. You can specify a number 1 - 9999.

MOUNTRetention
: Specifies the number of minutes to retain an idle connection with the target server before the connection is closed. This parameter is optional. You can specify a number 0 - 9999.
Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTLimit
: Specifies the maximum number of simultaneous sessions between the source server and the target server. Any attempts to access more sessions than indicated by the mount limit cause the requester to wait. This parameter is optional. You can specify a number 1 - 4096.
The following are possible values:

  number

Specifies the maximum number of simultaneous sessions between the source server and the target server.

1

Specifies the number of simultaneous sessions between the source server and the target server.

UPDATE DEVCLASS (Update a VOLSAFE device class)

Use the VOLSAFE device type to work with StorageTek VolSafe brand media and drives. This technology uses media that cannot be overwritten. Therefore, do not use these media for short-term backups of client files, the server database, or export tapes.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name--------------------------->

>--+--------------------------+--+--------------------------+--->
   '-LIBRary--=--library_name-'  '-FORMAT--=--+-DRIVE-----+-'
                                              +-9840------+
                                              +-9840-C----+
                                              +-T9840C----+
                                              +-T9840C-C--+
                                              +-T9840D----+
                                              +-T9840D-C--+
                                              +-T10000A---+
                                              +-T10000A-C-+
                                              +-T10000B---+
                                              +-T10000B-C-+
                                              +-T10000C---+
                                              +-T10000C-C-+
                                              +-T10000D---+
                                              '-T10000D-C-'

>--+---------------------+-------------------------------------->
   '-ESTCAPacity--=--size-'

>--+---------------------------------+----------------------->
   '-PREFIX--=--+-ADSM---------------+-'
                '-tape_volume_prefix-'

>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+--------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-number-+
                    '-0------'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be updated. The maximum length of the device class name is 30 characters.

LIBRary
: Specifies the name of the defined library object that contains the VolSafe drives that can be used by this device class. If any drives in a library are VolSafe-enabled, all drives in the library must be VolSafe-enabled. For more information about the VolSafe device type, see DEFINE DEVCLASS (Define a VOLSAFE device class).

FORMAT
: Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.
: Attention: If you specify DRIVE for a device class that has non-compatible sequential access devices, then you must mount volumes on devices that are capable of reading or writing the format that is established when the volume was first mounted. This can cause delays if the only sequential access device that can access the volume is already in use.
: The following table lists the recording formats and estimated capacities for VolSafe devices:

Table 1. Recording formats and default estimated capacities for volsafe tapes

Format	Estimated Capacity	Description
DRIVE	–	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library that contains some drives that support recording formats superior to other drives.
9840	20 GB	Uncompressed (standard) format, using a 20 GB cartridge with 270 meters (885 feet) of tape
9840-C	80 GB	LZ-1 Enhanced (4:1) compressed format, using an 80 GB cartridge with 270 meters (885 feet) of tape
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

ESTCAPacity

Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate due to compression of data.

You must specify this value as an integer followed by one of the following unit indicators: `K` (kilobytes), `M` (megabytes), `G` (gigabytes), or `T` (terabytes). The smallest value that is accepted is 1 MB (ESTCAPACITY=1M).

For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G.

To force the IBM Spectrum Protect™ server to determine the estimated capacity for the volumes that are assigned to this device class, specify ESTCAPACITY="".

For more information about the default estimated capacity for cartridge tapes, see Table 1.

PREFIX

Specifies the beginning portion of the high-level archive file name on the target server. This parameter is optional. The maximum length of this prefix is 8 characters.

If you have a naming convention for media labels to support your current management system, use a volume prefix that conforms to your naming conventions.

Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a high-level archive file name that uses the default prefix is ADSM.volume1.

MOUNTRetention
: Specifies the number of minutes that an idle sequential access volume is retained before it is dismounted. This parameter is optional. You can specify a number 0 - 9999.

  This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

  However, for EXTERNAL library types (that is, a library that is managed by an external media management system), set this parameter to a low value (for example, two minutes) to enhance device sharing between applications.

  Note: For environments in which devices are shared across storage applications, the MOUNTRETENTION setting must be carefully considered. This parameter determines how long an idle volume remains in a drive. Some media managers do not dismount an allocated drive to satisfy pending requests. You might need to tune this parameter to satisfy competing mount requests while maintaining optimal system performance. Typically, problems arise more frequently when the MOUNTRETENTION parameter is set to a value that is too small, for example, zero.

MOUNTWait
: Specifies the maximum number of minutes the server waits for an operator to respond to a request to either mount a volume in a drive in a manual library or check in a volume to be mounted in an automated library. This parameter is optional. If the mount request is not satisfied within the specified amount of time, the mount request is canceled. You can specify a number 0 - 9999.
  Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
: Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional. You can specify a number 0 - 4096.

  If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

  The following are possible values:

  DRIVES
  : Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.
    Note: For EXTERNAL library types, do not specify DRIVES for the MOUNTLIMIT value. Specify the number of drives for the library as the MOUNTLIMIT value.

  number
  : Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class.

  0 (zero)
  : Specifies that no new transactions can gain access to the storage pool. Any current transactions continue and complete, but new transactions are terminated.

AIX | Linux

UPDATE DEVCLASS - z/OS media server (Update device class for z/OS media server)

Use this command to update a device class. A limited set of device class types is available for devices that are accessed through a z/OS® media server.

- UPDATE DEVCLASS (Update a 3590 device class for z/OS media server)

- UPDATE DEVCLASS (Update a 3592 device class for z/OS media server)
- UPDATE DEVCLASS (Update an ECARTRIDGE device class for z/OS media server)
- UPDATE DEVCLASS (Update a FILE device class for z/OS media server)

Table 1. Commands related to UPDATE DEVCLASS

Command	Description
BACKUP DEVCONFIG	Backs up IBM Spectrum Protect device information to a file.
DEFINE DEVCLASS (z/OS media server)	Defines a device class to use storage managed by a z/OS media server.
DEFINE LIBRARY	Defines an automated or manual library.
DELETE DEVCLASS	Deletes a device class.
QUERY DEVCLASS	Displays information about device classes.
UPDATE LIBRARY	Changes the attributes of a library.

AIX Linux

UPDATE DEVCLASS (Update a 3590 device class for z/OS media server)

Use this command to update a device class that you defined to use a z/OS® media server to access 3590 devices. The device class that targets storage for the z/OS media server requires a library definition of type ZOSMEDIA.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

Notes:

1. You must specify at least one optional parameter on this command.

2. You cannot update the PREFIX parameter with this command. You must create a device class with the value that you require for the PREFIX parameter.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated.

LIBRary

Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

This parameter is optional.

For information about defining a library, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The following table lists the recording format options for 3590 devices:

Table 1. Recording formats for 3590

Format	Description
3590B	Uncompressed (basic) format
3590C	Compressed format
3590E-B	Uncompressed (basic) format, similar to the 3590B format
3590E-C	Compressed format, similar to the 3590C format
3590H-B	Uncompressed (basic) format, similar to the 3590B format
3590H-C	Compressed format, similar to the 3590C format
Note: If the format uses the tape drive hardware compression feature the actual capacity can increase, depending on the effectiveness of compression.	

ESTCAPacity
Specifies the estimated capacity for the sequential access volumes that are categorized by this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

COMPression
Specifies whether file compression is used for this device class. This parameter is optional.
You can specify one of the following values:

Yes
Specifies that the data for each tape volume is compressed.

No
Specifies that the data for each tape volume is not compressed.

MOUNTRetention
Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. Specify a number, 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait

Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

This parameter is optional. Specify a number, 1 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

You can specify one of the following values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
Specifies that no new transactions can gain access to the storage pool.

EXPiration
Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

Tip: You can specify a value of zero for this parameter. However, do so only if you also want to specify a value for the EXPIRATION parameter. You cannot specify a value for the EXPIRATION parameter if you specify a non-zero value for the RETENTION parameter.

PROtection
Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. You can specify one of the following values:

No
Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive,

allocation of tapes fails.

Automatic
: Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the server.

  The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

  Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

  If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

  Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT
: Specifies an esoteric unit name to specify a group of tape devices that support 3590 tape. This parameter is optional. The unit name can be up to 8 characters.

AIX Linux

UPDATE DEVCLASS (Update a 3592 device class for z/OS media server)

Use this command to update a device class that you defined to use a z/OS® media server to access 3592 devices. The device class that targets storage for the z/OS media server requires a library definition of type ZOSMEDIA.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
                                        (1)  (2)
>>-UPDate DEVclass--device_class_name-------------------------->

>--+-------------------------------+--------------------------->
   '-LIBRary--=--zos_media_library-'

>--+-------------------------+--+----------------------+--------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--size-'
                +-3592----+
                +-3592C---+
                +-3592-2--+
                +-3592-2C-+
                +-3592-3--+
                +-3592-3C-+
                +-3592-4--+
                '-3592-4C-'

>--+-------------------------+--------------------------------->
```

```
   '-COMPression--=--+-Yes-+-'
                     '-No--'

>--+---------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+---------------------------+--+-----------------------+---->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-EXPiration--=--yyyyddd-'
                    +-number-+
                    '-0------'

>--+--------------------+--+------------------------------+----->
   '-RETention--=--days-'  '-PROtection--=--+-No--------+-'
                                            +-Yes-------+
                                            '-Automatic-'

>--+--------------------+-----------------------------------><
   '-UNIT--=--unit_name-'
```

Notes:

1. You must specify at least one optional parameter on this command.
2. You cannot update the PREFIX parameter with this command. You must create a device class with the value that you require for the PREFIX parameter.

Parameters

device_class_name (Required)
Specifies the name of the device class to be updated. The maximum length of the device class name is 30 characters.

LIBRary

Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

This parameter is optional.

For information about defining a library, see the DEFINE LIBRARY command.

FORMAT
Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. The default value is DRIVE.
See the following table for the recording formats.

Table 1. Recording formats for 3592

Format	Description
3592	Uncompressed (basic) format
3592C	Compressed format
3592-2	Uncompressed (basic) format, similar to the 3592 format
3592-C	Compressed format, similar to the 3592C format
3592-3	Uncompressed (basic) format, similar to the 3592 format
3592-3C	Compressed format, similar to the 3592C format
3592-4	Uncompressed (basic) format, similar to the 3592 format
3592-4C	Compressed format, similar to the 3592C format
DRIVE	The server selects the highest format that is supported by the drive on which a volume is mounted. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library containing some drives that support recording formats superior to other drives.
Note: If this format uses the tape drive hardware compression feature, depending on the effectiveness of compression, the actual capacity might be different from the listed value.	

If the drives are in a library that includes drives of different tape technology, do not use the DRIVE value. Use the specific format that the drives use. For optimal results, do not mix generations of drives in the same library. If a library contains mixed generations, media problems can result. For example, generation 1 and generation 2 drives cannot read generation 3 media. If possible, upgrade all drives to 3592 generation 3. If you cannot upgrade all drives to 3592 generation 3, you must use a special configuration.

ESTCAPacity
Specifies the estimated capacity for the volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

COMPression
Specifies whether file compression is used for this device class. This parameter is optional. The default value is YES. You can specify one of the following values:

Yes
Specifies that the data for each tape volume is compressed.

No
Specifies that the data for each tape volume is not compressed.

MOUNTRetention
Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. Specify a number, 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait
Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

This parameter is optional. Specify a number, 1 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

You can specify one of the following values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
Specifies that no new transactions can gain access to the storage pool.

EXPiration
Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

Tip: You can specify a value of zero for this parameter. However, do so only if you also want to specify a value for the EXPIRATION parameter. You cannot specify a value for the EXPIRATION parameter if you specify a non-zero value for the RETENTION parameter.

PROtection
Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. You can specify one of the following values:

No
Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Automatic
Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the server.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT
: Specifies an esoteric unit name to specify a group of tape devices that support 3592 tape. This parameter is optional. This name can be as many as 8 characters.

AIX | Linux

UPDATE DEVCLASS (Update an ECARTRIDGE device class for z/OS media server)

Use this command to update a device class that you defined to use a z/OS® media server to access StorageTek drives such as the StorageTek T9840 or T10000. The device class that targets storage for the z/OS media server requires a library definition of type ZOSMEDIA.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
                                        (1) (2)
>>-UPDate DEVclass--device_class_name--------------------------->

>--+-------------------------------+---------------------------->
   '-LIBRary--=--zos_media_library-'

>--+---------------------------+--+----------------------+------->
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--size-'
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

>--+-----------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--minutes-'  '-MOUNTWait--=--minutes-'

>--+---------------------------+--+-------------------------+--->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-number-+                     '-No--'
                    '-0------'

>--+-----------------------+--+--------------------+----------->
   '-EXPiration--=--yyyyddd-'  '-RETention--=--days-'

>--+-------------------------------+--+--------------------+---><
   '-PROtection--=--+-No---------+-'  '-UNIT--=--unit_name-'
                    +-Yes-------+
                    '-Automatic-'
```

Notes:

1. You must specify at least one optional parameter on this command.
2. You cannot update the PREFIX parameter with this command. You must create a device class with the value that you require for the PREFIX parameter.

Parameters

device_class_name (Required)

Specifies the name of the device class to be updated.

LIBRary

Specifies the name of a library that was defined with the LIBTYPE=ZOSMEDIA parameter. The library and the tape drives that can be used by this device class are controlled by the z/OS media server.

This parameter is optional.

For information about defining a library, see the DEFINE LIBRARY command.

FORMAT

Specifies the recording format to be used when data is written to sequential access media. This parameter is optional. See the following table for the recording formats.

Table 1. Recording formats for ECARTRIDGE tapes

Format	Estimated Capacity	Description
DRIVE	-	The server selects the highest format that is supported by the drive on which a volume is mounted. DRIVE is the default value. Attention: Avoid specifying DRIVE when a mixture of drives is used within the same library. For example, do not use this option for a library containing some drives that support recording formats superior to other drives.
T9840C	40 GB	Uncompressed T9840C format, using a StorageTek 9840 cartridge
T9840C-C	80 GB	Compressed T9840C format, using a StorageTek 9840 cartridge
T9840D	75 GB	Uncompressed T9840D format, using a StorageTek 9840 cartridge
T9840D-C	150 GB	Compressed T9840D format, using a StorageTek 9840 cartridge
T10000A	500 GB	Uncompressed T10000A format, using a StorageTek T10000 cartridge
T10000A-C	1 TB	Compressed T10000A format, using a StorageTek T10000 cartridge
T10000B	1 TB	Uncompressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000B-C	2 TB	Compressed T10000B format, using an Oracle StorageTek T10000 cartridge
T10000C	5 TB	Uncompressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000C-C	10 TB	Compressed T10000C format, using an Oracle StorageTek T10000 T2 cartridge
T10000D	8 TB	Uncompressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge
T10000D-C	15 TB	Compressed T10000D format, using an Oracle StorageTek T10000 T2 cartridge

Note:

- Some formats use a compression feature of the tape drive hardware. Depending on the effectiveness of compression, the actual capacity might be double or more than the listed value.
- T10000A drives can read and write the T10000A format only. T10000B drives can read, but cannot write, the T10000A format. T10000C drives can read, but cannot write, the T10000A and T10000B formats. T10000D drives can read, but cannot write, the T10000A, T10000B, and T10000C formats.

ESTCAPacity

Specifies the estimated capacity for the sequential access volumes that are assigned to this device class. This parameter is optional.

You can specify this parameter if the default estimated capacity for the device class is inaccurate because of compression of data. The value does not determine the amount of data stored on the volume. The server uses the value to estimate the usage before a volume is filled. After a volume is full, the actual amount of data stored on the tape is used for the usage calculation.

Specify the value as an integer with one of the following unit indicators: `K` (KB), `M` (MB), `G` (GB), or `T` (TB). For example, specify that the estimated capacity is 9 GB with the parameter ESTCAPACITY=9G. The smallest value that is accepted is 100 KB (ESTCAPACITY=100K).

MOUNTRetention

Specifies the number of minutes that an idle tape volume is retained before it is dismounted. The time span for mount retention begins after the idle timeout period has expired. This parameter is optional. Specify a number, 0 - 9999.

This parameter can improve response time for sequential access media mounts by leaving previously mounted volumes online.

MOUNTWait
Specifies the maximum number of minutes that the z/OS media server waits for a volume mount. If the mount request is not satisfied within the specified time, the mount request fails. If a device is successfully allocated and the device-open request does not complete within the specified time, the device-open request ends and the mount request fails.

This parameter is optional. Specify a number, 1 - 9999.

Restriction: If the library that is associated with this device class is external (LIBTYPE=EXTERNAL), do not specify the MOUNTWAIT parameter.

MOUNTLimit
Specifies the maximum number of sequential access volumes that can be simultaneously mounted for the device class. This parameter is optional.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

You can specify one of the following values:

DRIVES
Specifies that every time a mount point is allocated, the number of drives that are defined and online in the library is used to calculate the true value.

number
Specifies the maximum number of drives in this device class that are used concurrently by the server. This value must never exceed the number of drives that are defined and online in the library that services this device class. You can specify a number, 0 - 4096.

0 (zero)
Specifies that no new transactions can gain access to the storage pool.

COMPression
Specifies whether file compression is used for this device class. This parameter is optional.
You can specify one of the following values:

Yes
Specifies that the data for each tape volume is compressed.

No
Specifies that the data for each tape volume is not compressed.

EXPiration
Specifies the expiration date that is placed on the tape labels for this device class. This parameter is optional.

Specify the date when the server no longer requires the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

Specify the expiration date using the format, *yyyyddd* (four digits for the year and three digits for the day). For example, January 7, 2014 is specified as `2014007` (the seventh day of year 2014).

If you specify the EXPIRATION parameter, you cannot specify the RETENTION parameter.

RETention
Specifies the number of days to retain the tape. This parameter is optional.

Specify the number of days (1 - 9999) that the server is expected to use the tape. The server does not use this information, but this information is passed to the z/OS media server for use by z/OS or tape management systems.

If you specify the RETENTION parameter, you cannot specify the EXPIRATION parameter.

Tip: You can specify a value of zero for this parameter. However, do so only if you also want to specify a value for the EXPIRATION parameter. You cannot specify a value for the EXPIRATION parameter if you specify a non-zero value for the RETENTION parameter.

PROtection

Specifies whether the RACF® program, if installed, protects volumes that are assigned to this device class. If protection is provided, RACF profiles are created when volumes are first used. This parameter is optional. You can specify one of the following values:

No

Specifies that the RACF program does not protect volumes that are assigned to this device class.

Yes

Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes, but the profiles are not deleted when volumes are deleted from the server. Profiles must be manually deleted.
Tip: If sensitive data is stored on volumes that are assigned to this device class, use PROTECTION=YES and manually delete RACF profiles only after tape volumes have been erased.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Automatic

Specifies that the RACF program protects volumes that are assigned to this device class. RACF profiles are created for volumes when the server first uses the volumes. RACF profiles are deleted when volumes are deleted from the server.

The profiles that are created for volumes depend on the system RACF settings. The protection that is provided is the same as using PROTECT=YES in JCL. If the RACF program is active and both TAPEVOL and TAPEDSN are inactive, allocation of tapes fails.

Important: If you specify PROTECTION=AUTOMATIC, when a volume is deleted, its RACF profile is deleted. The volume therefore is no longer protected by the RACF program. The data on these volumes can be accessed by other users.

If you specify PROTECTION=AUTOMATIC, the z/OS media server issues RACROUTE commands to delete profiles when a volume is deleted from the server. The deletion commands that are issued depend on the current system settings for TAPEVOL and TAPEDSN. If the system settings are changed, the z/OS media server might not delete existing profiles.

Do not change the setting to PROTECTION=AUTOMATIC for a device class that was set to PROTECTION=NO. Volumes without profiles might exist and error messages are generated when such volumes are deleted. If a different value for PROTECTION is required, define a new device class.

Profile creation and deletion occur based on the protection setting when the volume is first used and when it is deleted. The server does not attempt to create profiles for volumes that it has already used. If protection is set to AUTOMATIC, the server attempts to delete profiles when volumes are deleted.

See the documentation for the RACF program for details about the TAPEVOL and TAPEDSN settings and the profiles that are created when these settings are active.

UNIT

Specifies an esoteric unit name to specify a group of tape devices that support ECARTRIDGE tapes. Use the unit name that represents the subset of drives in the library that are attached to the z/OS system. This parameter is optional. The unit name can be up to 8 characters.

AIX | Linux

UPDATE DEVCLASS (Update a FILE device class for z/OS media server)

Use this command to update a device class that you defined to use a z/OS® media server to access files on magnetic disk storage as sequential-access volumes (like tape). The device class that targets storage for the z/OS media server requires a library definition of type ZOSMEDIA.

A volume in this device class is a Virtual Storage Access Method (VSAM) linear data set that is accessed by the z/OS media server. SCRATCH volumes can be used with a device class and the z/OS media server dynamically allocates the VSAM LDS. It is not necessary to define volumes for the server to use the device class. If you define volumes, set the high-level qualifier (HLQ) so that SMS recognizes the allocation request by the z/OS media server. If you are using defined volumes, the format volume function is

not supported for the server when you use this device class. The z/OS media server z/OS media server uses a FormatWrite feature of DFSMS Media Manager when filling FILE volumes.

You can define volumes for the FILE device class by using the DEFINE VOLUME command. However, the z/OS media server does not allocate space for a defined volume until the volume is opened for its first use.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DEVclass--device_class_name--------------------------->

>--+---------------------+--+---------------------+---------->
   '-MAXCAPacity--=--size-'  '-PRIMARYalloc--=--size-'

>--+-------------------------+--------------------------------->
   '-SECONDARYalloc--=--size-'

>--+-------------------------------+---------------------------->
   '-PREFIX--=--file_volume_prefix-'

>--+----------------------+---------------------------------><
   '-MOUNTLimit--=--number-'
```

Parameters

device_class_name (Required)
: Specifies the name of the device class to be defined. The maximum length of the device class name is 30 characters.

MAXCAPacity
: Specifies the maximum size of file volumes that are defined to a storage pool in this device class. This parameter is optional.

  Specify this value as an integer followed by `K` (KB), `M` (MB), `G` (GB), or `T` (TB). The minimum size is 1 MB (MAXCAPACITY=1M). The maximum size is 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc
: Specifies the initial amount of space that is dynamically allocated when a new volume is opened. Enough space must be available to satisfy the primary allocation amount. Storage Management Subsystem (SMS) policy determines whether multiple physical volumes can be used to satisfy the primary allocation request.

  This parameter is optional. Specify this value as an integer followed by `K` (KB), `M` (MB), `G` (GB), or `T` (TB). The minimum size is 100 KB (PRIMARYALLOC=100K). The maximum size is 16384 GB (MAXCAPACITY=16384G). All values are rounded to the next higher multiple of 256 KB.

  To avoid wasted space, the dynamic allocation operation uses the smaller of the values that are specified in the two parameters, PRIMARYALLOC and MAXCAPACITY.

  SMS automatic class selection (ACS) routines can affect whether the PRIMARYALLOC and SECONDARYALLOC parameter values are used.

SECONDARYalloc
: Specifies the amount of space by which a file volume is extended when space that is already allocated to the file volume is used up. The data set for a file volume is extended up to the size set by the MAXCAPACITY parameter, then the volume is marked full.

  Because secondary allocation of a linear data set cannot span a physical volume, consider the size of the physical volume when selecting a secondary allocation size. For example, physical volumes for a 3390 Model 3 are approximately 2.8 GB. To ensure that each extend request occupies nearly an entire physical volume but not more, use a secondary allocation size that is just less than 2.8 GB. A secondary allocation amount of 2600 MB allots enough space for the VSAM volume data set (VVDS), the volume label, and the volume table of contents (VTOC).

This parameter is optional. Specify this value as an integer followed by K (KB), M (MB), G (GB), or T (TB). The minimum value is 0 KB (SECONDARYALLOC=0K). The maximum value is 16384 GB. Except for 0, all values are rounded to the next higher multiple of 256 KB.

If you specify 0 (SECONDARYALLOC=0), the file volume cannot be extended beyond the primary allocation amount.

SMS automatic class selection (ACS) routines can affect whether the PRIMARYALLOC and SECONDARYALLOC parameter values are used.

If you specify a value for the SECONDARYALLOCATION parameter that is not 0, or if you allow the value to default to 2600M, the SMS DATACLAS associated with the PREFIX identifier (for example, High Level Qualifier) must have the Extended Addressability (EA) attribute specified. Without the EA attribute, the SMS DATACLAS limits the allocation of the VSAM LDS FILE volume to the primary extent. (See the description of the PRIMARYALLOCATION parameter). With the data set limited to primary allocation size, the data set cannot be extended by the z/OS media server, and the volume is marked FULL before the maximum capacity is reached.

Restriction: Ensure that the values that you specify for the PRIMARYALLOC and SECONDARYALLOC parameters are within practical limits for the storage device. The server cannot check whether the values exceed practical device limits, and does not check whether the two values together exceed the current MAXCAPACITY setting.
Tip: To fill volumes when you specify a large value for the MAXCAPACITY parameter, specify large values for the PRIMARYALLOC and SECONDARYALLOC parameters. Use larger MVS™ volume sizes to reduce the chance of extend failure.

PREFIX

Specifies the high-level qualifier of the data set name that is used to allocate scratch volume data sets. For all scratch file volumes created in this device class, the server uses this prefix to create the data set name. This parameter is optional. The maximum length of the prefix, including periods, is 32 characters.
Values that are specified for this parameter must meet the following conditions:

- The value is to be made up of qualifiers, which can be a maximum of eight characters including periods. For example, the following value is acceptable:

  ```
  AB.CD2.E
  ```

- The qualifiers must be separated by a single period.
- The first letter of each qualifier must be alphabetic or national (@,#,$), followed by alphabetic, national, hyphen, or numeric characters.

An example of a file volume data set name using the default prefix is `ADSM.B0000021.BFS`.

If you have a data set naming convention, use a prefix that conforms to your naming conventions. For example, the following value is acceptable: `TSM.SERVER2.VSAMFILE`.

If you are running multiple server instances for either IBM Spectrum Protect™ or Tivoli® Storage Manager for z/OS Media you must use a unique value for the PREFIX parameter for each device class that you update.

MOUNTLimit

Specifies the maximum number of FILE volumes that can be open concurrently for this device class. This parameter is optional. For 3995 devices emulating 3390 devices, the value must not be set higher than the numbers of concurrent input and output streams possible on the media storing the volumes.

The value that you specify in this parameter is important if there is a significant penalty switching from one volume to another. For example, switching can take place when using IBM® 3995 devices to emulate 3390 devices. The value that you specify must be no higher than the number of physical drives available on the device.

If you plan to use the simultaneous-write function, ensure that sufficient drives are available for the write operation. If the number of drives needed for a simultaneous-write operation is greater than the value of the MOUNTLIMIT parameter for a device class, the transaction fails.

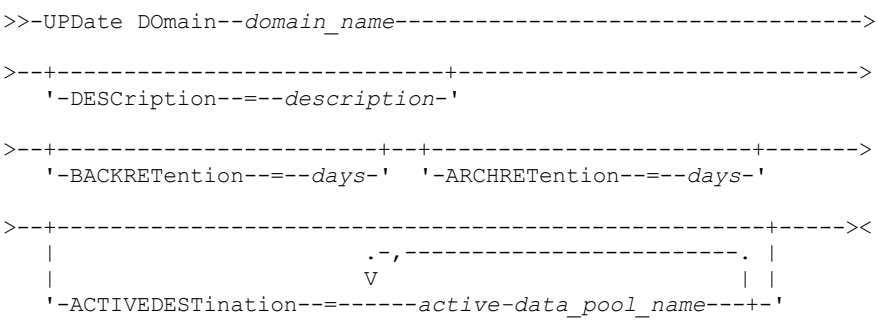
UPDATE DOMAIN (Update a policy domain)

Use this command to change a policy domain.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the specified policy domain.

Syntax



Parameters

domain_name (Required)
: Specifies the name of the policy domain.

DESCription
: Describes the policy domain by using a text string. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove a previously defined description, specify a null string ("").

BACKRETention
: Specifies the number of days (from the date the backup versions became inactive) to retain backup versions that are no longer on the client file system. This parameter is optional. You can specify an integer in the range 0 - 9999. The server uses the backup retention value to manage inactive versions of files when any of the following conditions occur:

  - A file is rebound to a new management class, but the new management class and the default management class do not contain a backup copy group.
  - The management class to which a file is bound no longer exists. The default management class does not contain a backup copy group.
  - The backup copy group is deleted from the management class to which a file is bound. The default management class does not contain a backup copy group.

ARCHRETention
: Specifies the number of days (from the date of archive) to retain archive copies. This parameter is optional. You can specify an integer in the range 0 - 30000. The server uses the archive retention value to manage archive copies of files when either of the following conditions occur:

  - The management class to which a file is bound, no longer exists. The default management class does not contain an archive copy group.
  - The archive copy group is deleted from the management class to which a file is bound. The default management class does not contain an archive copy group.

ACTIVEDESTination
: Specifies the names of active-data pools that store active versions of backup data for nodes that are assigned to the domain. This parameter is optional. Spaces between the names of the active-data pools are not permitted. You cannot specify more than 10 active-data pools for a domain.

  Before the IBM Spectrum Protect™ server writes data to an active-data pool, it verifies that the node that owns the data is assigned to a domain that has the active-data pool that is listed in the ACTIVEDESTINATION list. If the server verifies that the node meets this criteria, the data is stored in the active-data pool. If the node does not meet the criteria, then the data is not stored in the active-data pool. If the simultaneous-write function is used to write data to an active-data pool, the server completes the verification during backup operations by IBM Spectrum Protect backup-archive clients or by application clients by using the IBM Spectrum Protect API. The verification is also done when active-data is being copied by using the COPY ACTIVEDATA command.

Example: Update the backup retention period for a policy domain

Update the policy domain ENGPOLDOM so that the backup retention grace period is extended to 90 days and the archive retention grace period is extended to two years. Specify an active-data pool as the destination for active versions of backup data belonging to nodes that are assigned to the domain. Use *engactivedata* as the name of the active-data pool. Issue the following command:

```
update domain engpoldom description='Engineering Policy Domain'
backretention=90 archretention=730 activedestination=engactivedata
```

Related commands

Table 1. Commands related to UPDATE DOMAIN

Command	Description
COPY DOMAIN	Creates a copy of a policy domain.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE DOMAIN	Deletes a policy domain along with any policy objects in the policy domain.
QUERY DOMAIN	Displays information about policy domains.

UPDATE DRIVE (Update a drive)

Use this command to update a drive.

Privilege class

For detailed and current drive support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate DRive--library_name--drive_name----------------------->

>--+-------------------------------+--+--------------------+----->
   '-SERial--=--+-serial_number-+-'  '-ONLine--=--+-Yes-+-'
                '-AUTODetect----'                 '-No--'

>--+-----------------------------+-------------------------------->
   '-ELEMent--=--+-address----+-'
                 '-AUTODetect-'

>--+--------------------------+--------------------------------->
   |                      (1) |
   '-ACSDRVID--=--drive_id-----'

>--+-----------------------------------------+----------------><
   |                     (2)                 |
   '-CLEANFREQuency--=------+-NONE----------+-'
                            |          (3) |
                            +-ASNEEDED-----+
                            '-gigabytes----'
```

Notes:

1. The ACSDRVID parameter is valid only for drives in ACSLS libraries.
2. The CLEANFREQUENCY parameter is valid only for drives in SCSI libraries.
3. The CLEANFREQUENCY=ASNEEDED parameter value does not work for all tape drives. For more information, see the parameter description.

Parameters

library_name (Required)
Specifies the name of the library to which the drive is assigned.

drive_name (Required)
Specifies the name that is assigned to the drive.

SERial
Specifies the serial number for the drives that are being updated. This parameter is valid only for drives in a SCSI or virtual tape library (VTL). This parameter is optional. The possible values are:

serial_number
Specifies the serial number for the drive that is being updated.
Note: If a path to this drive is already defined, then the number you enter here is compared to the number detected by IBM Spectrum Protect™. If the numbers do not match, the command fails.

AUTODETECT
Specifies that the serial number is automatically detected and used by IBM Spectrum Protect if a path is already defined to this drive.

If a path to this drive is not defined, then the serial number is not detected.

ONLine
Specifies whether the drive is available for use. This parameter specifies whether drives can be taken offline and used for another activity, such as maintenance. This parameter is optional.

You can issue this command when the drive is involved in an active process or session, but it is not advised. If you issue a command to take the drive offline while it is in use, an error message is issued. The mounted volume completes its current process. If this volume was part of a series of volumes for a specific transaction, the drive is not available to complete mounting the series. If no other drives are available, the process fails.

Attention: When a drive is in use, do not specify the ELEMENT parameter with the ONLINE parameter. The drive is not updated, and the command fails.

The drive state is not changed even if the server is halted and restarted. If a drive is offline when the server is restarted, a warning message is issued stating that the drive must be manually brought online. If all of the drives in a library are updated to be offline, processes that need a library mount point fail, rather than queue up for a mount point.

YES
Specifies that the drive is available for use (online).

No
Specifies that the drive is not available for use (offline).

ELEMent
Specifies the element address of the drive within a SCSI or VTL library. The server uses the element address to connect the physical location of the drive to the SCSI address of the drive. This parameter is valid only for a drive in a SCSI or VTL library when the command is issued from an IBM Spectrum Protect library manager server. The possible values are:

address
Specifies the element address for the drive that is being updated.

To find the element address for your library configuration, consult the information from the manufacturer.

Remember: If a path to this drive is already defined, then the number you enter here is compared to the number previously detected by IBM Spectrum Protect. If the numbers do not match, then this command fails.

AUTODETECT
Specifies that the element number is automatically detected and used by IBM Spectrum Protect if a path is already defined to this drive.

If a path to this drive is not defined, then the element number is not detected.

Restriction: If the library in which the drive is located does not support the Read Element Status SCSI command, and ELEMENT=AUTODETECT, the command fails with an IBM Spectrum Protect error message.

ACSDRVID
Specifies the ID of the drive that is being accessed in an ACSLS library. The drive ID is a set of numbers that indicates the physical location of a drive within an ACSLS library. This drive ID must be specified as *a,l,p,d,* where *a* is the ACSID, *l* is the

LSM (library storage module), *p* is the panel number, and *d* is the drive ID. The server needs the drive ID to connect the physical location of the drive to the drive's SCSI address. See your StorageTek documentation for details.

CLEANFREQuency

Specifies how often the server activates drive cleaning. This parameter is optional. For the most complete automation of cleaning for an automated library, you must have a cleaner cartridge checked into the volume inventory for the library. If you are using library based cleaning, NONE is advised when your library type supports this function. This parameter is valid only for drives in SCSI libraries, and not valid for externally managed libraries, such as 3494 libraries or StorageTek libraries that are managed under ACSLS.

Important: There are special considerations if you plan to use server-activated drive cleaning with a SCSI library that provides automatic drive cleaning support in its device hardware.

NONE

Specifies that the server does not track cleaning for this drive. Use this parameter for libraries that have their own automatic cleaning.

ASNEEDED

Specifies that the server loads the drive with a checked-in cleaner cartridge only when a drive reports to the device driver that it needs cleaning.

The CLEANFREQUENCY=ASNEEDED parameter value does not work for all tape drives. Visit the Supported Devices website for your operating system to view detailed drive information. If ASNEEDED is not supported, you can use the gigabytes value for automatic cleaning.

For IBM 3592 and LTO drives, library based cleaning is advised. If library based cleaning is not supported, then ASNEEDED must be used. Gigabytes is not recommended.

Restriction: IBM Spectrum Protect does not control the drives that are connected to the NAS file server. If a drive is attached only to a NAS file server (no connection to a storage agent or server), do not specify ASNEEDED for the cleaning frequency.

gigabytes

Specifies, in gigabytes, how much data is processed on the drive before the server loads the drive with a cleaner cartridge. The server resets the gigabytes-processed counter each time it loads a cleaner cartridge in the drive.

Important: When CLEANFREQUENCY=gigabyte, drive cleaning can occur before the gigabyte setting is reached, if the drive notifies the device driver that a cleaning is necessary.

Consult the information from the drive manufacturer for cleaning recommendations. If the information gives recommendations for cleaning frequency in terms of hours of use, convert to a gigabytes value by doing the following:

1. Use the bytes-per-second rating for the drive to determine a gigabytes-per-hour value.
2. Multiply the gigabytes-per-hour value by the recommended hours of use between cleanings.
3. Use the result as the cleaning frequency value.

Tip: For IBM 3590, specify a value for the cleaning frequency to ensure that the drives receive adequate cleaning. Consult the information from the drive manufacturer for cleaning recommendations. Using the cleaning frequency that is recommended by IBM does not over clean the drives.

Example: Update the element address for a drive

Update DRIVE3, in the library named AUTO, by changing the element address to 119.

```
update drive auto drive3 element=119
```

Example: Take a drive offline

Update DRIVE3, in the library named MANLIB, to take it offline.

```
update drive manlib drive3 online=no
```

Related commands

Table 1. Commands related to UPDATE DRIVE

Command	Description
CLEAN DRIVE	Marks a drive for cleaning.

Command	Description
DEFINE DRIVE	Assigns a drive to a library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DRIVE	Deletes a drive from a library.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
UPDATE PATH	Changes the attributes associated with a path.

UPDATE FILESPACE (Update file-space node-replication rules)

Use this command to update file-space replication rules. You can also enable or disable replication of data to which a file space rule applies.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node with the file space to be updated belongs.

Syntax

Notes:

1. You cannot specify a file space identifier (FSID) if you use wildcard characters for the client node name.
2. You can specify each rule only once.
3. You must specify either the REPLRULE or the REPLSTATE parameter on this command.
4. The ACTIVE_DATA and ACTIVE_DATA_HIGH_PRIORITY rules are valid only if you specify `DATATYPE=BACKUP`.

Parameters

node_name (Required)
: Specifies the client node to which the file space belongs. You can use wildcard characters to specify this name. However, file space identifiers can be different among client nodes for the same file space. Therefore, you cannot specify wildcard characters for the client node name and FSID as the value for the NAMETYPE parameter.

file_space_name (Required)

: Specifies the name of the file space to be updated. You can use wildcard characters or a comma-delineated list to specify names.

: For a server that has clients with Unicode-enabled file spaces, you might have to make the server convert the file space name that you enter. For example, you might have to make the server convert a name from the server code page to Unicode. For details, see the NAMETYPE parameter. If you specify only a single wildcard character for the name, you can use the CODETYPE parameter to limit the operation to Unicode file spaces or to non-Unicode file spaces.

: File space names are case-sensitive. To determine the correct capitalization for the file space to be updated, use the QUERY FILESPACE command.

NAMEType
: Specifies how you want the server to interpret the file space names that you enter. You can use this parameter for IBM Spectrum Protect™ clients that Unicode-enabled and that have Windows, Macintosh OS X, or NetWare operating systems. Use this parameter only when you enter a partly-qualified or fully-qualified file space name. The default value is SERVER. You can specify one of the following values:

: SERVER
: The server uses the server code page to interpret file space names.

: UNIcode
: The server converts file space names from the server code page to the UTF-8 code page. The success of the conversion depends on the operating system, on the characters in the name, and the server code page. Conversion can fail if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion fails, the name can contain question marks, blanks, or ellipses (...).

: FSID
: The server interprets file space names as file space identifiers.

CODEType
: Specifies the type of file spaces to be included in node replication processing. The default value is BOTH, meaning that file spaces are included regardless of code page type. Use this parameter only when you enter a single wildcard character for the file space name. You can specify one of the following values:

: UNIcode
: Specifies only file spaces that are in Unicode.

: NONUNIcode
: Specifies only file spaces that are not in Unicode.

: BOTH
: Specifies all file spaces regardless of code page type.

DATAType (Required)
: Specifies the data type to which a replication rule applies. To specify multiple data types, separate the names with commas and no intervening spaces. You can specify the following values:

: BACKup
: Specifies the backup data type.

: ARCHive
: Specifies the archive data type.

: SPACEManaged
: Specifies the space-managed data type.

REPLRule

Specifies the replication rule that applies to a data type. You cannot use wildcards. If you specify multiple data types, the replication rule applies to each data type. For example, if you specify `DATATYPE=BACKUP,ARCHIVE`, the replication rule applies to backup data and to archive data.
Restriction: The REPLRULE parameter is optional. However, if you do not specify it, you must specify the REPLSTATE parameter.

You can specify normal-priority replication or high-priority replication rules. In a replication process that includes both normal and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

For example, suppose that a file space contains active backup data and archive data. Replication of the active backup data is a higher priority than the archive data. To prioritize the active backup data, specify `DATATYPE=BACKUP REPLRULE=ACTIVE_DATA_HIGH_PRIORITY`. To assign a normal priority to archive data, issue the UPDATE FILESPACE command again, and specify `DATATYPE=ARCHIVE REPLRULE=ALL_DATA`.

You can specify the following rules:

ALL_DATA
: Replicates backup, archive, or space-managed data. The data is replicated with a normal priority.

ACTIVE_DATA
: Replicates only the active backup data in a file space. The data is replicated with a normal priority.
Attention: If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

  - When a server version earlier than Version 7.1.1 is installed on either the source or target replication servers.
  - When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
  - When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a server version earlier than V7.1.1.

  If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
: Replicates backup, archive, or space-managed data. The data is replicated with a high priority.

ACTIVE_DATA_HIGH_PRIORITY

: This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority.

DEFAULT
: Data is replicated according to the client node rule for the data type.

  For example, suppose that you want to replicate the archive data in all the file spaces that belong to a client node. Replication of the archive data is a high priority. One method to accomplish this task is to specify `DATATYPE=ARCHIVE REPLRULE=DEFAULT` for each file space. Ensure that the client replication rule for archive data is set to ALL_DATA_HIGH_PRIORITY or to DEFAULT. If the client replication rule is DEFAULT, the server replication rule for archive data must be set to ALL_DATA_HIGH_PRIORITY.

NONE
: Data is not replicated. For example, if you do not want to replicate the space-managed data in a file space, specify `DATATYPE=SPACEMANAGED REPLRULE=NONE`.

REPLState
: Specifies the replication state for a data type. If you specified multiple data types, the state applies to all the data types. For example, if you specified `DATATYPE=BACKUP,ARCHIVE`, the state applies to backup data and archive data.

  The REPLSTATE parameter is optional. However, if you do not specify it, you must specify the REPLRULE parameter. You can specify one of the following values for the REPLSTATE parameter:

  ENabled
  : Specifies that the data type is ready for replication.

  DISabled
  : Specifies that replication does not occur until you enable it.

  PURGEdata
  : Specifies that data is deleted from the target replication server. The type of data deleted is the type of data specified by the DATATYPE parameter. For example, if you specify `DATATYPE=BACKUP,ARCHIVE` and `REPLSTATE=PURGEDATA`, backup data and archive data are deleted from the file space on the target replication server.

After the data is deleted, the REPLSTATE parameter is set to DISABLED, preventing future replication of the data type or types. The replication rule for the data type is set to DEFAULT.

Remember: PURGEDATA processing does not delete file spaces. Only data is deleted. The file space shows as empty in the output of the QUERY OCCUPANCY command.

Example: Update replication rules for two data types

NODE1 has three file spaces: /a, /b, and /c. The replication rules for all file spaces are set to ALL_DATA. However, you want to replicate the backup and archive data in file space /a before the data in other file spaces is replicated.

```
update filespace node1 /a datatype=backup,archive replrule=
       all_data_high_priority
```

Example: Update replication rules for two data types

NODE2 has two file spaces: /a and /b. You want to temporarily suspend replication of all data in file space /b.

```
update filespace node2 /b datatype=backup,archive,spacemanaged
 replstate=disabled
```

Related commands

Table 1. Commands related to UPDATE FILESPACE

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET REPLRETENTION	Specifies the retention period for replication history records.
UPDATE NODE	Changes the attributes that are associated with a client node.
UPDATE REPLRULE	Enables or disables replication rules.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

UPDATE LIBRARY (Update a library)

Use this command to update a library definition.

AIX Windows To update the device name, the ACS number, or the external manager path name of a library, you must use the UPDATE PATH command.

Linux To update the device name or the external manager path name of a library, you must use the UPDATE PATH command.

Syntax and parameter descriptions are available for the following library types.

- UPDATE LIBRARY (Update a 349X library)
- UPDATE LIBRARY (Update an ACSLS library)
- UPDATE LIBRARY (Update an EXTERNAL library)
- UPDATE LIBRARY (Update a FILE library)
- UPDATE LIBRARY (Update a manual library)
- UPDATE LIBRARY (Update a SCSI library)
- UPDATE LIBRARY (Update a shared library)
- UPDATE LIBRARY (Update a VTL library)

For detailed and current library support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Windows

To automatically label tape volumes in SCSI-type libraries, use the AUTOLABEL parameter on the DEFINE LIBRARY and UPDATE LIBRARY commands. Using this parameter eliminates the need to pre-label a set of tapes. It is also more efficient than using the LABEL LIBVOLUME command, which requires you to mount volumes separately. If you use the AUTOLABEL parameter, you must check in tapes by specifying CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

A label cannot include embedded blanks or periods and must be valid when used as a file name on the media.

You must label CD-ROM, Zip, or Jaz volumes with the device utilities from the manufacturer or the Windows utilities because IBM Spectrum Protect™ does not provide utilities to format or label these media types. The operating system utilities include the Disk Administrator program (a graphical user interface) and the label command.

Related commands

Table 1. Commands related to UPDATE LIBRARY

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE DRIVE	Deletes a drive from a library.
DELETE LIBRARY	Deletes a library.
DELETE PATH	Deletes a path from a source to a destination.
LABEL LIBVOLUME	Labels volumes in manual or automated libraries.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DRIVE	Changes the attributes of a drive.
UPDATE LIBVOLUME	Changes the status of a storage volume.
UPDATE PATH	Changes the attributes associated with a path.

UPDATE LIBRARY (Update a 349X library)

Use this syntax to update a 349X library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name--+--------------------+--------->
                                 '-SHAREd--=----Yes---'
```

```
>--+-------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+----------------------------->
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

>--+-------------------------------+-------------------------><
   '-WORMSCRatchcategory--=--number-'
```

Parameters

library_name (Required)
: Specifies the name of the library to be updated.

SHAREd
: Specifies that this library is shared with other servers in a storage area network (SAN). You must issue this command from the server defined as the primary library manager for the shared library. This parameter is required for libraries defined to a library manager and for libraries used for NDMP operations. Specify SHARED=YES to update a library that is not currently shared.
Important: If a library has a path from a data mover (such as a NAS file server) but no connection to the server, the library cannot be shared with another server.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
: Specifies that the server does not attempt to label any volumes.

Yes
: Specifies that the server only labels unlabeled volumes.

OVERWRITE
: Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

WORMSCRatchcategory
: Specifies the category number to be used for WORM scratch volumes in the library. This parameter is required if you use WORM volumes. You can specify a number from 1 to 65279. This number must be unique. It cannot be shared with other applications or defined libraries, and it must be different from the other category numbers in this library. This parameter is only valid when 3592 WORM volumes are used.
Restriction: This parameter can only be updated if the device class WORM parameter is set to YES and the WORMSCRATCHCATEGORY currently has no defined value.

RESETDrives
: Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established.

AIX Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

The following table describes the three possible configurations for drives that are attached to NAS devices.

Table 1. Configurations for drives that are attached to NAS devices.

Library device configuration	The behavior for persistent reserve

Library device configuration	The behavior for persistent reserve
The library device is attached to the IBM Spectrum Protect server, and the tape drives are shared by the server and the NAS device.	Drive reservation preemption is supported when the NAS device supports persistent reserve and it is enabled. For more information about setting persistent reserve, see the documentation for your NAS device.
The library device is attached to the IBM Spectrum Protect server and the tape drives are accessed only from the NAS device.	Drive reservation preemption is not supported. If you enable persistent reserve on the NAS device for these drives and a reservation is set by the NAS device but never cleared, you must use another method to clear the reservation.

AIX Windows

Yes
: Specifies that drive preemption through persistent reserve or target reset are used.

No
: Specifies that drive preemption through persistent reserve or target reset are not used. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
: Specifies that drive preemption through persistent reserve is used.

No
: Specifies that drive preemption through persistent preserve is not used.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

Example: Add new devices to a shared library

Update a 3494 shared library named 3494LIB2 with new device names. AIX Linux

```
update library 3494lib2 device=/dev/lmcp1,/dev/lmcp2,/dev/lmcp3
```

Windows

```
update library 3494lib device=lb3.0.0.0,lb4.0.0.0,lb5.0.0.0
```

UPDATE LIBRARY (Update an ACSLS library)

Use this syntax to update an ACSLS library.

Privilege class

Windows In order to use ACSLS functions, the installation of StorageTek Library Attach software is required.

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name--+--------------------+--------->
                                 '-SHAREd--=----Yes---'

>--+------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+--+------------------+------><
   '-AUTOLabel--=--+-No--------+-'  '-ACSID--=--number-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameters

library_name (Required)
Specifies the name of the library to be updated.

SHAREd
Specifies that this library is shared with other servers in a storage area network (SAN). You must issue this command from the server defined as the primary library manager for the shared library. This parameter is required for libraries defined to a library manager and for libraries used for NDMP operations. Specify SHARED=YES to update a library that is not currently shared.
Important: If a library has a path from a data mover (such as a NAS file server) but no connection to the server, the library cannot be shared with another server.

RESETDrives
Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established.

AIX Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

The following table describes the three possible configurations for drives that are attached to NAS devices.

Table 1. Configurations for drives that are attached to NAS devices.

Library device configuration	**The behavior for persistent reserve**
The library device is attached to the IBM Spectrum Protect server, and the tape drives are shared by the server and the NAS device.	Drive reservation preemption is supported when the NAS device supports persistent reserve and it is enabled. For more information about setting persistent reserve, see the documentation for your NAS device.
The library device is attached to the IBM Spectrum Protect server and the tape drives are accessed only from the NAS device.	Drive reservation preemption is not supported. If you enable persistent reserve on the NAS device for these drives and a reservation is set by the NAS device but never cleared, you must use another method to clear the reservation.

AIX Windows

Yes
Specifies that drive preemption through persistent reserve or target reset are used.

No
Specifies that drive preemption through persistent reserve or target reset are not used. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
Specifies that drive preemption through persistent reserve is used.

No
Specifies that drive preemption through persistent preserve is not used.

Note: A library manager will not be able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

AUTOLabel
Specifies whether the server attempts to automatically label tape volumes. This parameter is optional.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
Specifies that the server does not attempt to label any volumes.

Yes
Specifies that the server only labels unlabeled volumes.

OVERWRITE

Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

ACSID (Required)
Specifies the number of this StorageTek library assigned by the ACSSA (Automatic Cartridge System System Administrator). This can be a number from 0 to 126. Issue QUERY ACS on your system to get the number for your library ID. This parameter is required.

See your StorageTek documentation for more information.

Example: Update an ID number for an ACSLS library

Update an ACSLS library named ACSLSLIB with a new ID number.

```
update library acslslib acsid=1
```

UPDATE LIBRARY (Update an EXTERNAL library)

Use this syntax to update an external library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name---------------------------------->

>--+-----------------------------+----------------------------><
   '-AUTOLabel--=--+-No---------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameters

library_name (Required)
Specifies the name of the library to be updated.

AUTOLabel
Specifies whether the server attempts to automatically label tape volumes. This parameter is optional.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
Specifies that the server does not attempt to label any volumes.

Yes
Specifies that the server only labels unlabeled volumes.

OVERWRITE
Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

Example: Update the path name for an external library

Update an external library named EXTLIB with a new path name for the media manager. AIX Linux

```
update library extlib externalmanager=/v/server/mediamanager
```

Windows

```
update library extlib externalmanager=c:\server\mediamanager
```

UPDATE LIBRARY (Update a FILE library)

Use this syntax to update a FILE library

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name--+--------------------+--------><
                                 '-SHAREd--=----Yes---'
```

Parameters

library_name (Required)
: Specifies the name of the library to be updated.

SHAREd
: Specifies that this library is shared with other servers in a storage area network (SAN). You must issue this command from the server defined as the primary library manager for the shared library. This parameter is required for libraries defined to a library manager and for libraries used for NDMP operations. Specify SHARED=YES to update a library that is not currently shared.

  Important: If a library has a path from a data mover (such as a NAS file server) but no connection to the server, the library cannot be shared with another server.

Example: Update a FILE library to be shared

Update a file library named FILE2, so that it is shared:

```
update library file2 shared=yes
```

UPDATE LIBRARY (Update a manual library)

Use this syntax to update a manual library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name--+-------------------------+---->
                                 '-RESETDrives--=--+-Yes-+-'
                                                   '-No--'

>--+-----------------------------+----------------------------><
   '-AUTOLabel--=---+-No--------+-'
                    +-Yes-------+
                    '-OVERWRITE-'
```

Parameters

library_name (Required)
: Specifies the name of the library to be updated.

RESETDrives
: Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established.

  AIX | Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

  Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect™ device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

AIX | Windows

Yes
: Specifies that drive preemption through persistent reserve or target reset are used.

No
: Specifies that drive preemption through persistent reserve or target reset are not used. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
: Specifies that drive preemption through persistent reserve is used.

No
: Specifies that drive preemption through persistent preserve is not used.

Note: A library manager is not able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

AUTOLabel
: Specifies whether the server attempts to automatically label tape volumes. This parameter is optional.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
: Specifies that the server does not attempt to label any volumes.

Yes
: Specifies that the server labels only unlabeled volumes.

OVERWRITE
: Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

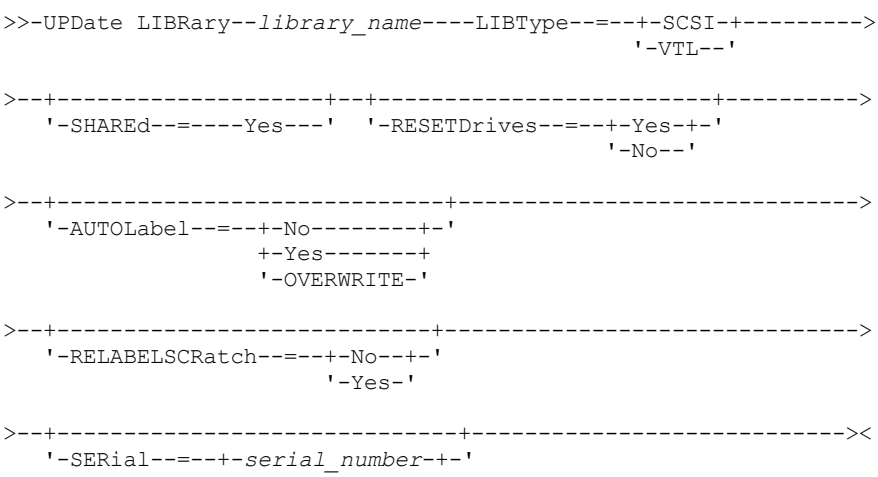
UPDATE LIBRARY (Update a SCSI library)

Use this syntax to update a SCSI library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



```
'-AUTODetect----'
```

Parameters

library_name (Required)
: Specifies the name of the library to be updated.

LIBType (Required)
: Specifies the library type that you want to update to. Possible values are:

  VTL
  : Specifies that the library has a SCSI-controlled media changer device that is represented by a Virtual Tape Library. To mount volumes on drives in this type of library, IBM Spectrum Protect™ uses the media changer device. This value is effective when specified for libraries with a current library type of SCSI.
  Note: Selecting the VTL library type assumes that the following conditions are true:

  - Your environment does not include mixed-media
  - Paths are defined between all drives in the library and all defined servers, including storage agents, that use the library

  If both conditions are not met, performance can degrade to the same levels as the SCSI library type especially during times of high stress when most drives are in use concurrently.

  SCSI
  : Specifies that the library has a SCSI-controlled media changer device. To mount volumes on drives in this type of library, IBM Spectrum Protect uses the media changer device. This value is effective when specified for libraries with a current library type of VTL.

SHAREd
: Specifies that this library is shared with other servers in a storage area network (SAN). You must issue this command from the server defined as the primary library manager for the shared library. This parameter is required for libraries defined to a library manager and for libraries used for NDMP operations. Specify SHARED=YES to update a library that is not currently shared.
Important: If a library has a path from a data mover (such as a NAS file server) but no connection to the server, the library cannot be shared with another server.

RESETDrives
: Specifies whether the server preempts a drive reservation if the drive is already reserved by persistent reserve when the server tries to access the drive.

  AIX Windows If the drive is reserved by a SCSI-2 reserve, (and not by persistent reserve), the server uses a LUN reset to break the drive reservation to access the target device.

  Linux LUN resets are not supported by the Linux operating system. If a drive is reserved by a SCSI-2 reserve, (and not by persistent reserve), the server is unable to break the reservation to access the drive. In this case, you can break the reservation by power cycling the device.

  For Network-Attached Storage (NAS) devices, reservation is controlled by the NAS file server. IBM Spectrum Protect does not control NAS devices and the RESETDrives parameter is not relevant for NAS devices.

  Support for persistent reserve has the following limitations:

  - If you are using the IBM Spectrum Protect device driver, persistent reserve is supported only on some tape drives. For details, see Technote 1470319.
  - If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. For information about driver configuration, see the *IBM Tape Device Drivers Installation and User's Guide*.
  - If you are using a virtual tape library that is emulating a supported drive, persistent reserve might not be supported.

  AIX Windows

  Yes
  : Specifies that drive preemption through persistent reserve or target reset is used.

  No
  : Specifies that drive preemption through persistent reserve or target reset is not used. The RESETDrives parameter must be set to YES in a clustered environment when SHARED=NO.

  Linux

Yes
Specifies that drive preemption through persistent reserve is used.

No
Specifies that drive preemption through persistent preserve is not used.

AUTOLabel
Specifies whether the server attempts to automatically label tape volumes.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
Specifies that the server does not attempt to label any volumes.

Yes
Specifies that the server only labels unlabeled volumes.

OVERWRITE
Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

SERial
Specifies the serial number for the library being updated. This parameter is optional. The possible values are:

serial_number
Specifies the serial number for the library being updated.

If a path to this library has already been defined, then the number you enter here is compared to the number detected by IBM Spectrum Protect. If the numbers do not match, the command fails. If a path has not been defined, this serial number is verified when a path is defined.

AUTODetect
Specifies that the serial number is automatically detected and used by IBM Spectrum Protect if a path has already been defined to this library.

If a path to this library has not been defined, then the serial number is not detected.

RELABELSCRatch
Specifies whether the server relabels volumes that have been deleted and returned to scratch. When this parameter is set to YES, a LABEL LIBVOLUME operation is started and the existing volume label is overwritten. This parameter is optional and intended for use with a Virtual Tape Library (VTL).
Note: If you have both virtual and real volumes in your VTL, both types are relabeled when this parameter is enabled. If the VTL includes real volumes, specifying this option might affect performance.

No
Specifies that the server does not relabel volumes that are deleted and returned to scratch.

Yes
Specifies that the server relabels volumes that are deleted and returned to scratch.

UPDATE LIBRARY (Update a shared library)

Use this syntax to update a shared library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBRary--library_name---------------------------------->

>--PRIMarylibmanager--=--server_name--------------------------><
```

Parameters

library_name (Required)
Specifies the name of the library to be defined. The maximum length of this name is 30 characters.
PRIMarylibmanager
Specifies the name of the server that is responsible for controlling access to library resources. You must define this server with the DEFINE SERVER command before you can use it as a library manager.

Example: Change the library manager server for a library

For a library client server, change the name of the library manager server to CASTOR.

```
update library ltolib primarylibmanager=castor
```

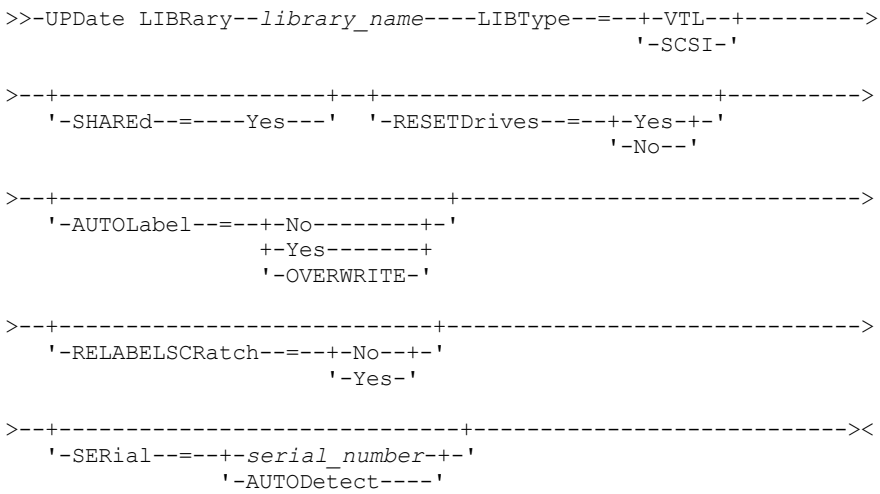
UPDATE LIBRARY (Update a VTL library)

Use this syntax to update a library that is defined as VTL.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

library_name (Required)
Specifies the name of the library to be defined. The maximum length of this name is 30 characters.
LIBType (Required)
Specifies the type of library that is being defined. Possible values are:

SCSI
Specifies that the library has a SCSI-controlled media changer device. To mount volumes on drives in this type of library, IBM Spectrum Protect™ uses the media changer device. This value is effective when specified for libraries with a current library type of VTL.
VTL
Specifies that the library has a SCSI-controlled media changer device that is represented by a Virtual Tape Library. To mount volumes on drives in this type of library, IBM Spectrum Protect uses the media changer device. This value is effective when specified for libraries with a current library type of SCSI.
Note: Select the VTL library type only if the following conditions are true:

- Your environment does not include mixed-media
- Paths are defined between all drives in the library and all defined servers, including storage agents, that use the library

If both conditions are not met, performance can degrade to the same levels as the SCSI library type especially during times of high stress when most drives are in use concurrently.

SHAREd
Specifies that this library is shared with other servers in a storage area network (SAN). You must issue this command from the server defined as the primary library manager for the shared library. This parameter is required for libraries defined to a library manager and for libraries used for NDMP operations. Specify SHARED=YES to update a library that is not currently shared.
Important: If a library has a path from a data mover (such as a NAS file server) but no connection to the server, the library cannot be shared with another server.

RESETDrives
Specifies whether the server preempts a drive reservation with persistent reserve when the server is restarted or when a library client or storage agent reconnection is established.

AIX Windows If persistent reserve is not supported, the server completes a reset of the path to the target device.

Linux If persistent reserve is not supported, the server is not able to reset the path to the target device.

Support for persistent reservation has the following limitations:

- If you are using the IBM Spectrum Protect device driver, persistent reserve is only supported on some tape drives. See Technote 1470319 for details.
- If you are using the IBM® device driver, persistent reserve must be enabled at the device driver level. See the *IBM Tape Device Drivers Installation and User's Guide* for information about driver configuration.
- If you are using a virtual tape library that is emulating a supported drive, it might not support persistent reserve.

AIX Windows

Yes
Specifies that drive preemption through persistent reserve or target reset are used.

No
Specifies that drive preemption through persistent reserve or target reset are not used. The RESETDRIVES parameter must be set to YES in a clustered environment when SHARED=NO.

Linux

Yes
Specifies that drive preemption through persistent reserve is used.

No
Specifies that drive preemption through persistent preserve is not used.

Note: A library manager is not able to break a drive reservation if the system that has the drive reservation is not configured to use persistent reservation.

AUTOLabel
Specifies whether the server attempts to automatically label tape volumes. This parameter is optional.

To use this option, you must check in the tapes with CHECKLABEL=BARCODE on the CHECKIN LIBVOLUME command.

No
Specifies that the server does not attempt to label any volumes.

Yes
Specifies that the server only labels unlabeled volumes.

OVERWRITE
Specifies that the server attempts to overwrite an existing label. The server overwrites existing labels *only* if both the existing label and the bar code label are not already defined in any server storage pool or volume history list.

RELABELSCRatch
Specifies whether the server relabels volumes that have been deleted and returned to scratch. When this parameter is set to YES, a LABEL LIBVOLUME operation is started and the existing volume label is overwritten.
Note: If you have both virtual and real volumes in your VTL, both types are relabeled when this parameter is enabled. If the VTL includes real volumes, specifying this option might affect performance.

Yes
Specifies that the server relabels volumes that are deleted and returned to scratch.

No
Specifies that the server does not relabel volumes that are deleted and returned to scratch.

SERial
Specifies the serial number for the library being updated. This parameter is optional. The possible values are:

serial_number
Specifies the serial number for the library being updated.

If a path to this library has already been defined, then the number you enter here is compared to the number detected by IBM Spectrum Protect. If the numbers do not match, then the command fails. If a path has not been defined, this serial number is verified when a path is defined.

AUTODetect
Specifies that the serial number is automatically detected and used by IBM Spectrum Protect if a path has already been defined to this library.

If a path to this library has not been defined, then the serial number is not detected.

UPDATE LIBVOLUME (Change the status of a storage volume)

Use this command to change the status of a sequential access storage volume in a library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate LIBVolume--library_name--volume_name--STATus--=--+-PRIvate-+-->
                                                           '-SCRatch-'

>--+----------------------+-----------------------------------><
   '-OWNer--=--server_name-'
```

Parameters

library_name (Required)
Specifies the name of the library.

volume_name (Required)
Specifies the volume name of the storage volume.

STATus (Required)
Specifies a change to the status of a storage volume. Possible values are as follows:

PRIvate
Specifies that the server updates the storage volume to a private volume.

SCRatch
Specifies that the server updates the storage volume to a scratch volume.

Restriction: You cannot change the status of a volume from private to scratch if the volume belongs to a storage pool or is defined in the volume history file. You can change the status if you make a mistake when you check in volumes to the library and assign the volumes the wrong status.

AIX Linux Windows OWNer

AIX Linux Windows Specifies which server owns a private volume in a shared library that is shared across a SAN. You can change the owner of a private volume in a shared library (SAN) when you issue the command from the library manager server. If you do not specify this parameter, the library manager server owns the private volume.
Important: Do not use OWNER as a value for scratch volumes. However, you can use OWNER when you change a scratch volume to private.

Example: Update a volume's status

Update the volume that is named WPDV00 in the library that is named AUTO to reflect a status of PRIVATE.

```
update libvolume auto wpdv00 status=private
```

Related commands

Table 1. Commands related to UPDATE LIBVOLUME

Command	Description
AUDIT LIBRARY	Ensures that an automated library is in a consistent state.
CHECKIN LIBVOLUME	Checks a storage volume into an automated library.
CHECKOUT LIBVOLUME	Checks a storage volume out of an automated library.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
AIX Linux Windows LABEL LIBVOLUME	AIX Linux Windows Labels volumes in manual or automated libraries.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY LIBVOLUME	Displays information about a library volume.

UPDATE MACHINE (Update machine information)

Use this command to update machine information. This information will be included in the plan file to help you to recover the client machines.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UPDate MACHine--machine_name---------------------------------->

>--+------------------------------+--+----------------------+--->
   '-DESCription--=--description-'  '-BUilding--=--building-'

>--+-----------------+--+---------------+----------------------->
   '-FLoor--=--floor-'  '-ROom--=--room-'

>--+---------------------+--+-----------------------+---------><
   '-PRIority--=--number-'  '-ADSMServer--=--+-Yes-+-'
                                             '-No--'
```

Parameters

machine_name (Required)
: Specifies the name of the machine to be updated.

DESCription
: Specifies a description of the machine. This parameter is optional. The text can be up to 255 characters. Enclose the text in quotation marks if it contains any blank characters. To remove existing text, specify a null string ("").

BUilding
: Specifies the name or number of the building that this machine is in. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters. To remove existing text, specify a null string ("").

FLoor
: Specifies the name or number of the floor that this machine is on. This parameter is optional. The text can be up to16 characters. Enclose the text in quotation marks if it contains any blank characters. To remove existing text, specify a null string ("").

ROom
: Specifies the name or number of the room that this machine is in. This parameter is optional. The text can be up to 16 characters. Enclose the text in quotation marks if it contains any blank characters. To remove existing text, specify a null string ("").

PRIority
: Specifies the restore priority for the machine as an integer from 1 to 99. The highest priority is 1. This parameter is optional. Use this value to prioritize client machine recovery.

ADSMServer
: Specifies whether the machine contains an IBM Spectrum Protect™ server. This parameter is optional. Possible values are:

  No
  : This machine does not contain an IBM Spectrum Protect server.

  Yes
  : This machine contains an IBM Spectrum Protect server. Only one machine can be defined as containing an IBM Spectrum Protect server.

Example: Update information for a specific machine

Update the DISTRICT5 machine information to reflect that it contains the server.

```
update machine district5 adsmserver=yes
```

Related commands

Table 1. Commands related to UPDATE MACHINE

Command	Description
DEFINE MACHINE	Defines a machine for DRM.
DELETE MACHINE	Deletes a machine.
INSERT MACHINE	Inserts machine characteristics or recovery instructions into the IBM Spectrum Protect database.
QUERY MACHINE	Displays information about machines.

UPDATE MGMTCLASS (Update a management class)

Use this command to change a management class. To allow clients to use the updated management class, you must activate the policy set that contains the management class.

Important: The UPDATE MGMTCLASS command fails if a copy storage pool is specified as the destination for files that were migrated by an IBM Spectrum Protect™ for Space Management client.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-UPDate MGmtclass--domain_name--policy_set_name--class_name--->

>--+-------------------------------------+----------------------->
   '-SPACEMGTECHnique--=--+-AUTOmatic-+-'
                          +-SELective-+
                          '-NONE------'

>--+-------------------------+---------------------------------->
   '-AUTOMIGNonuse--=--days-'

>--+-----------------------------+------------------------------->
   '-MIGREQUIRESBkup--=--+-Yes-+-'
                         '-No--'

>--+-------------------------------+----------------------------->
   '-MIGDESTination--=--pool_name-'

>--+-----------------------------+------------------------------><
```

```
'-DESCription--=--description-'
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the management class belongs.

policy_set_name (Required)
: Specifies the policy set to which the management class belongs. You cannot update a management class that belongs to the ACTIVE policy set.

class_name (Required)
: Specifies the management class to update.

SPACEMGTECHnique
: Specifies whether a file using this management class is eligible for migration. This parameter is optional. This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients. Possible values are:

  AUTOmatic
  : Specifies that the file is eligible for both automatic migration and selective migration.

  SELective
  : Specifies that the file is eligible for selective migration only.

  NONE
  : Specifies that the file is not eligible for migration.

AUTOMIGNonuse
: Specifies the number of days that must elapse since a file was last used before it is eligible for automatic migration. This parameter is optional. If SPACEMGTECHNIQUE is not AUTOMATIC, the server ignores this attribute. You can specify an integer from 0 to 9999.

  This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients.

MIGREQUIRESBkup
: Specifies whether a backup version of a file must exist before a file can be migrated. This parameter is optional. This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients. Possible values are:

  Yes
  : Specifies that a backup version must exist.

  No
  : Specifies that a backup version is optional.

MIGDESTination
: Specifies the primary storage pool where the server initially stores files migrated by IBM Spectrum Protect for Space Management clients. This parameter is effective only for IBM Spectrum Protect for Space Management clients, not for backup-archive clients or application clients.

  The command fails if you specify a copy storage pool as the destination.

DESCription
: Specifies a description of the management class. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove a previously defined description, specify a null string ("").

Example: Update the policy domain and storage pool of a specific management class

For the management class ACTIVEFILES, in policy set VACATION in the EMPLOYEE_RECORDS policy domain, change the storage pool where migrated files are stored.

```
update mgmtclass employee_records vacation
activefiles migdestination=diskpool2
```

Related commands

Table 1. Commands related to UPDATE MGMTCLASS

Command	Description
ASSIGN DEFMGMTCLASS	Assigns a management class as the default for a specified policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE MGMTCLASS	Defines a management class.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE MGMTCLASS	Deletes a management class and its copy groups from a policy domain and policy set.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.
QUERY POLICYSET	Displays information about policy sets.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.

UPDATE NODE (Update node attributes)

Use this command to modify the attributes of a registered node.

You must use the RENAME NODE command to change the name of a registered node.

If you update the node authentication method or the node SSLREQUIRED setting and there is a same-named administrator, those administrator ID settings change.

You must have system level authority to update the node authentication method or the node SSLREQUIRED setting and also update a same-named administrator ID. If the same-named administrator ID has client owner authority over the node that is being updated, then system level authority is not required. You must have either unrestricted policy privilege or restricted policy privilege for the policy domain to which the client node belongs.

For users of Lightweight Directory Access Protocol (LDAP) servers:

- The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
- If you change the authentication mode to LDAP, and the node name matches an administrative user ID, you might see unexpected behavior when an automatic password change occurs because the password might be updated twice. As a result, the password might become unknown to the administrative user ID. Alternatively, the password update operation might fail.

When you register or update a node, you can specify whether damaged files on the node can be recovered from a target replication server. Files can be recovered only if all the following conditions are met:

- Version 7.1.1 or later, is installed on the source and target replication servers.
- The REPLRECOVERDAMAGED system parameter is set to ON. The system parameter can be set by using the SET REPLRECOVERDAMAGED command.
- The source server includes at least one file that is marked as damaged in the node that is being replicated.
- The node data was replicated before the damage occurred.

The following table describes how parameter settings affect the recovery of damaged, replicated files.

Table 1. Settings that affect the recovery of damaged files

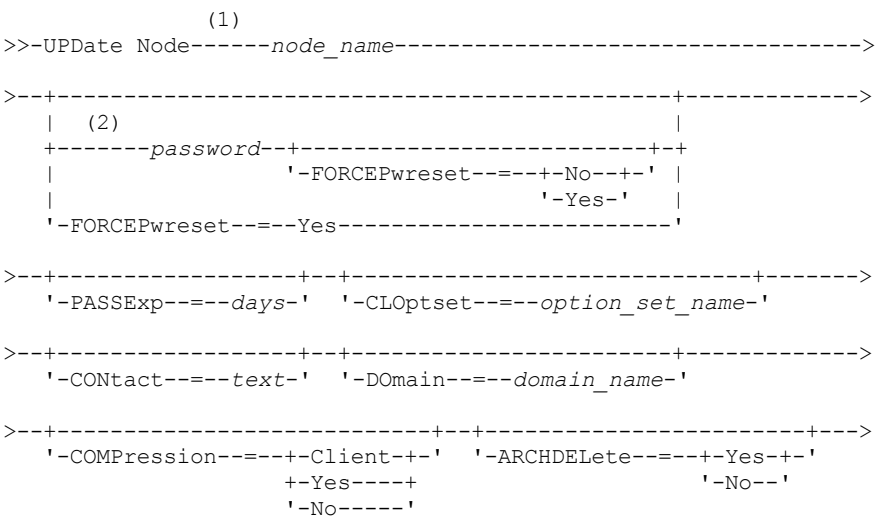
Setting for the REPLRECOVERDAMAGED system parameter	Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command	Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands	Result

Setting for the REPLRECOVERDAMAGED system parameter	Value of the RECOVERDAMAGED parameter on the REPLICATE NODE command	Value of the RECOVERDAMAGED parameter on the REGISTER NODE and UPDATE NODE commands	Result
OFF	YES, NO, or not specified	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
OFF	ONLY	YES or NO	An error message is displayed because files cannot be recovered when the REPLRECOVERDAMAGED system parameter is set to OFF.
ON	YES	YES or NO	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	NO	YES or NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.
ON	ONLY	YES or NO	Damaged files are recovered from the target replication server, but standard node replication does not occur.
ON	Not specified	YES	During node replication, standard replication occurs and damaged files are recovered from the target replication server.
ON	Not specified	NO	During node replication, standard replication occurs and damaged files are not recovered from the target replication server.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the client node belongs.

Syntax




'-BACKDELete--=--+-No--+-'
'-Yes-'
'-WHEREDOmain--=--domain_name-'
'-WHEREPLatform--=--client_platform_name-'
'-MAXNUMMP--=--number-'
'-KEEPMP--=--+-No--+-'
'-Yes-'
'-URL--=--url_address-'
'-UTILITYUrl--=--utility_url-'
(3)
'-AUTOFSRename--=--+-Yes----+-'
+-No-----+
'-Client-'
'-VALIdateprotocol--=--+-No-------+-'
+-Dataonly-+
'-All------'
'-TXNGroupmax--=--+-0------+-'
'-number-'
.-DATAWritepath--=--ANY---------.
'-DATAWritepath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
.-DATAReadpath--=--ANY---------.
'-DATAReadpath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
'-TARGETLevel--=--V.R.M.F-'
.-SESSIONINITiation--=--Clientorserver---.
'-SESSIONINITiation--=--+-Clientorserver---+-'
| (4) |
'-SERVEROnly--HLAddress--=--ip_address--LLAddress--=--tcp_port-----'
'-HLAddress--=--ip_address-'
| (4) |
'-LLAddress--=--tcp_port-----'
'-EMAILADdress--=--userID@node-'
'-DEDUPlication--=--+-SERVEROnly-----+-'
'-Clientorserver-'
| (5) |
'-BACKUPINITiation--=--+-All--+-----'
'-ROOT-'

Notes:

1. You must specify at least one optional parameter on this command.
2. Passwords are optional for this command, except when you change the authentication method from LDAP to LOCAL.
3. The VALIDATEPROTOCOL parameter is deprecated.
4. HLADDRESS and LLADDRESS must be previously set or specified in the UPDATE NODE or REGISTER NODE commands to use SESSIONINITIATION=SERVERONLY.
5. The BACKUPINITIATION parameter is ignored if the client node operating system is not supported.
6. If you specify the REPLSTATE parameter and you do not specify the REPLMODE parameter, the replication mode of the node is set to SEND.
7. If you specify the REPLMODE parameter, you must also specify the REPLSTATE parameter.

8. The SYNCLDAPDELETE parameter applies only if a node that authenticates to a Lightweight Directory Access Protocol (LDAP) server reverts to local authentication.
9. The SSLREQUIRED parameter is deprecated.

Parameters

node_name (Required)
Specifies the name of the client node to be updated. You can use wildcard characters to specify this name.
Restriction: When you update a password with the UPDATE NODE command, you cannot use a wildcard character with the `node_name` parameter.

password
Specifies the new password for the client node. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters. This parameter is optional in most cases. If the node authentication method is changed from LDAP to LOCAL, a password is required. If the node authentication method is LDAP, do not specify a password by using the UPDATE NODE command. Passwords remain current for a period that is determined by the password expiration period.

FORCEPwreset
Specifies whether to force a client to change or reset the password. This parameter is optional. You can specify one of the following values:

No
Specifies that the password expiration period is set by the SET PASSEXP command. Do not force a client to change or reset the password while it attempts to log on to the server.

Yes
Specifies that the client node or administrator password will expire at the next logon. The client must change or reset the password at the next logon.
Restrictions:

- For nodes that authenticate with an LDAP server, password expiration is set by using LDAP server utilities. For this reason, do not specify FORCEPWRESET=YES if you plan to specify AUTHENTICATION=LDAP.
- If you plan to update a node to authenticate with an LDAP server, and you specified FORCEPWRESET=YES, you must change the password before you can specify FORCEPWRESET=NO and AUTHENTICATION=LDAP.

PASSExp
Specifies the number of days the password remains valid. You can set the password expiration period in the range 0 - 9999 days. A value of 0 means that the password never expires. This parameter is optional. If you do not specify this parameter, the password expiration period is unchanged.

You can change the password expiration period by using the UPDATE NODE or SET PASSEXP commands. To set a common expiration period for all administrators and client nodes, issue the SET PASSEXP command. You can also use the SET PASSEXP command to selectively set password expiration periods. If you selectively set a password expiration period by using the REGISTER NODE command, the UPDATE NODE command, or the SET PASSEXP command, the expiration period is excluded from common password expiration periods that were created by using the SET PASSEXP command.

You can use the RESET PASSEXP command to reset the password expiration period to the common expiration period. This parameter does not apply to passwords that authenticate with an LDAP directory server.

CLOptset
Specifies the name of the option set to be used by the client. This parameter is optional. To remove a client option set, specify the CLOPTSET parameter with a null string ("").

CONtact
Specifies a text string of information that identifies the client node. This parameter is optional. The maximum length of the text string is 255 characters. Enclose the contact information in quotation marks if it contains any blanks. To remove previously defined contact information, specify a null string ("").

DOmain
Specifies the name of the policy domain to which you want to register the client node. This parameter is optional.
Restriction: For servers with data retention protection enabled, an archived registered node cannot be reassigned to a different policy domain.

COMPression

Specifies whether the client node compresses its files before it sends them to the server for backup and archive. This parameter is optional.
Restriction: This parameter cannot be specified for a NAS node.

You can specify one of the following values:

Client
: Specifies that the client determines whether files are to be compressed.

Yes
: Specifies that the client node compresses its files before it sends them to the server for backup and archive.

No
: Specifies that the client node does not compress its files before it sends them to the server for backup and archive.

ARCHDELete
: Specifies whether the client node can delete its own archived files from the server. This parameter is optional. You can specify one of the following values:

Yes
: Specifies that the client node can delete its own archive files from the server.

No
: Specifies that the client node cannot delete its own archive files from the server.

BACKDELete
: Specifies whether the client node can delete its own backup files from the server. This parameter is optional. You can specify one of the following values:

No
: Specifies that the client node cannot delete its own backup files from the server.

Yes
: Specifies that the client node can delete its own backup files from the server.

WHEREDOmain
: Specifies the name of the policy domain to be used as a filter in combination with the node name to select nodes to update. This parameter is optional.

WHEREPLatform
: Specifies the name of the client platform to be used as a filter in combination with the node name to select nodes to update. This parameter is optional.

MAXNUMMP
: Specifies the maximum number of mount points a node can use on the server or storage agent only for operations such as backup, archive, and IBM Spectrum Protect for Space Management migration. The parameter is optional and does not apply to nodes with a type of NAS or SERVER. The default value is 1. You can specify an integer in the range 0 - 999. A value of 0 specifies that a node cannot acquire any mount point for a client data store operation. The MAXNUMMP value is not evaluated or enforced during client data read operations such as restore, retrieve, and IBM Spectrum Protect for Space Management recall. However, mount points in use for data read operations are evaluated against attempted concurrent data store operations for the same client node and might prevent the data store operations from being able to acquire mount points.

  For volumes in a storage pool that is associated with the FILE or CENTERA device type, the server can have multiple sessions to read and one process to write to the same volume concurrently. To increase concurrency and provide efficient access for nodes with data in FILE or CENTERA storage pools, increase the value of the MAXNUMMP parameter.

  For nodes that store data into primary storage pools with the simultaneous-write function that is enabled, you must adjust the value of the MAXNUMMP parameter to specify the correct number of mount points for each client session. A client session requires one mount point for the primary storage pool and one mount point for each copy storage pool and each active-data pool.

URL
: Specifies the URL of the IBM Spectrum Protect web client that is configured on the client system. You can use the URL in a web browser and in the Operations Center to remotely manage the client node.

  This parameter is optional. The URL must include the DNS name or IP address of the client system, and the port number that is defined on the client system for the IBM Spectrum Protect web client. For example,
  `http://client.mycorp.com:1581`

If you want to remove the value from this parameter, specify empty single quotation marks or empty double quotation marks with no spaces ('' for single quotation marks, or "" for double quotation marks).

UTILITYUrl
Specifies the address of the IBM Spectrum Protect client management services that are configured on the client system. This URL is used by the Operations Center to access client log files so that you can remotely diagnose client issues from the Operations Center.

This parameter is optional. You can specify a URL of up to 200 characters in length. The URL must start with `https`. It includes the DNS name or IP address of the client system, and the port number that is defined on the client system for the IBM Spectrum Protect client management services. For example, `https://client.mycorp.com:9028`

If you omit the port number, the Operations Center uses the port number 9028, which is the default port number when you install the client management services on the client system.

KEEPMP
Specifies whether the client node keeps the mount point for the entire session. The parameter is optional. You can specify one of the following values:

No
Specifies that the client node releases the mount point during the session. If policy definitions cause data to be stored to a disk storage pool after data is stored to a sequential access storage pool, any mount points that are held by the session will be released.

Yes
Specifies that the client node must retain the mount point during the entire session. If policy definitions cause data to be stored to a disk storage pool after data is stored to a sequential access storage pool, any mount points that are held by the session will not be released.

AUTOFSRename
Specifies whether the client is prompted for renaming file spaces when the client system upgrades to a client that supports Unicode. The prompting and renaming, if allowed, occur only when the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup. The renaming changes the names of existing backed-up file spaces that are not in Unicode in server storage. Then, the file spaces are backed up in Unicode. You can use this parameter for Unicode-enabled IBM Spectrum Protect clients by using Windows, Macintosh OS X, and NetWare operating systems.
Important: After the client with support for Unicode is installed, any new file spaces that the client backs up are stored in server storage by using the UTF-8 code page. UTF-8 is a byte-oriented encoding form that is specified by the Unicode Standard.

You can specify one of the following values:

Yes
The server automatically renames existing file spaces when the client system upgrades to a client that supports Unicode, and the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup. The renaming occurs whether the client uses the graphical user interface, the command line, or the client scheduler.
For example, the server renames a drive as follows:

- Original name: D_DRIVE
- New name: D_DRIVE_OLD

The new name indicates that the file space is stored on the server in format that is not Unicode.

No
The server does not rename file spaces automatically when the client system upgrades to a client that supports Unicode, and the client runs one of the following operations: archive, selective backup, full incremental backup, or partial incremental backup.

Client
The option AUTOFSRENAME in the client option file determines whether file spaces are renamed.

By default, the client option is set to PROMPT. When the client system upgrades to a client that supports Unicode and the client runs an IBM Spectrum Protect operation with the graphical user interface or the command line, the program displays a one-time prompt to the user about whether to rename file spaces.

When the client scheduler runs an operation, the program does not prompt for a choice about renaming, and does not rename file spaces. Backups of existing file spaces are sent as before (not in Unicode).

VALIdateprotocol (deprecated)

Specifies whether IBM Spectrum Protect performs a cyclic redundancy check to validate the data that is sent between the client and the server. The parameter is optional.

Important: Beginning with IBM Spectrum Protect Version 8.1.2 and Tivoli® Storage Manager Version 7.1.8, this parameter is deprecated. The validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The VALIDATEPROTOCOL parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

TXNGroupmax

Specifies the number of files that are transferred as a group between a client and a server between transaction commit points. Client performance might be improved by using a larger value for this option.

Specifying 0 indicates that the node uses the server global value that is set in the server options file. To use a value other than the server global value, specify a value of 4 through 65,000 for this parameter. The node value takes precedence over the server value.

Tip: Increasing the TXNGROUPMAX value increases recovery log utilization. Higher recovery log utilization might increase the risk of running out of log space. Evaluate the performance of each node before you change the parameter.

DATAWritepath

Specifies the transfer path that is used when the client sends data to the server, storage agent, or both, during storage operations such as backup or archive. The parameter is optional.

Remember: If a path is unavailable, the node cannot send any data. For example, if you select the LAN-free option but a LAN-free path is not defined, the operation fails.

You can specify one of the following values:

ANY

Specifies that data is sent to the server, storage agent, or both, using any available path. A LAN-free path is used if one is available. If a LAN-free path is unavailable, the data is moved over the LAN.

LAN

Specifies that data is sent over the LAN.

LANFree

Specifies that data is sent over a LAN-free path.

DATAReadpath

Specifies the transfer path that is used when the server, storage agent, or both read data for a client, during operations such as restore or retrieve. The parameter is optional.

Remember: If a path is unavailable, data cannot be read. For example, if you select the LAN-free option but a LAN-free path is not defined, the operation fails. The value for the transfer path also applies to failover connections. If the value is set to LANFree, failover cannot occur for the node on the secondary server.

You can specify one of the following values:

ANY

Specifies that the server, storage agent, or both use any available path to read data. A LAN-free path is used if one is available. If a LAN-free path is unavailable, the data is read over the LAN.

LAN

Specifies that data is read over the LAN.

LANFree

Specifies that data is read by using a LAN-free path.

SESSIONINITiation

Controls whether the server or the client initiates sessions. The parameter is optional.

Clientorserver

Specifies that the client might initiate sessions with the server by communicating on the TCP/IP port that is defined with the server option TCPPORT. Server-prompted scheduling might also be used to prompt the client to connect to the server.

SERVEROnly

Specifies that the server does not accept client requests for sessions. All sessions must be initiated by server-prompted scheduling on the port that is defined for the client with the REGISTER or UPDATE NODE commands. You cannot use the client acceptor, dsmcad, to start the scheduler when SESSIONINITIATION is set to SERVERONLY.

HLAddress

Specifies the client IP address that the server contacts to initiate scheduled events. This parameter must be used when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that are previously used by the client to contact the server.

The address can be specified either in numeric or host name format. If a numeric address is used, it is saved without verification by a domain name server. If the address is not correct, it can cause failures when the server attempts to contact the client. Host name format addresses are verified with a domain name server. Verified names are saved and resolved with Domain Name Services when the server contacts the client.

LLAddress

Specifies the client port number on which the client listens for sessions from the server. This parameter must be used when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that are previously used by the client to contact the server.

The value for this parameter must match the value of client option TCPCLIENTPORT. The default value is 1501.

HLAddress

Specifies the client IP address that the server contacts to initiate scheduled events. This optional parameter is used only when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that were previously used by the client to contact the server. If SESSIONINITIATION SERVERONLY is not in use, this option has no effect.

The address can be specified either in numeric or host name format. If a numeric address is used, it is saved without verification by a domain name server. If the address is not correct, it can cause failures when the server attempts to contact the client. Host name format addresses are verified with a domain name server. Verified names are saved and resolved with Domain Name Services when the server contacts the client.

LLAddress

Specifies the client port number on which the client listens for sessions from the server. This optional parameter is used only when SESSIONINITIATION is set to SERVERONLY, regardless of any addresses that were previously used by the client to contact the server. If SESSIONINITIATION SERVERONLY is not in use, this option has no effect.

The value for this parameter must match the value of client option TCPCLIENTPORT. The default value is 1501.

EMAILADdress
This parameter is used for more contact information. The information that is specified by this parameter is not acted upon by IBM Spectrum Protect.

DEDUPlication
Specifies where data deduplication can occur for this node. You can specify one of the following values:

SERVEROnly
Specifies that data that is stored by this node can be deduplicated on the server only.

Clientorserver
Specifies that data that is stored by this node can be deduplicated on either the client or the server. For data deduplication to take place on the client, you must also specify a value of YES for the DEDUPLICATION client option. You can specify this option in the client option file or in the client option set on the IBM Spectrum Protect server.

TARGETLevel

Specifies the client deployment package that is targeted for this node. You can substitute an applicable release package for V.R.M.F (Version.Release.Modification.Fix) Level. For example: `TARGETLevel=6.2.0.0`.

You must specify each segment with a number that is applicable to a deployment package. You cannot use an asterisk in any field as a substitution for a valid number. To remove an existing value, specify a null string (" "). The parameter is optional.
Restriction: The TARGETLEVEL parameter does not apply to nodes with a type of NAS or SERVER.

BACKUPINITiation

Specifies whether the non-root user ID on the client node can back up files to the server. The parameter is optional. The default value is ALL, indicating that non-root user IDs can back up data to the server. You can select one of the following values:

All
: Specifies that non-root user IDs can back up files to the server. ALL is the default if BACKUPINITIATION is not specified.

ROOT
: Specifies that only the root user ID can back up files to the server.
Restriction: The attribute is ignored by the server if the backup-archive client connects from an operating system other than AIX®, Linux, or Mac OS.

BKREPLRuledefault, ARREPLRuledefault, and SPREPLRuledefault
: Specifies the replication rule that applies to a data type if the file space rules for the data type are set to DEFAULT:

BKREPLRuledefault
: Specifies the replication rule for backup data.

ARREPLRuledefault
: Specifies the replication rule for archive data.

SPREPLRuledefault
: Specifies the replication rule for space-managed data.

You can specify normal-priority replication or high-priority replication rules. In a replication process that includes both normal and high-priority data, high-priority data is replicated first. Before you specify a rule, consider the order in which you want the data to be replicated.

For example, suppose that a client node contains active backup data and archive data. Replication of the active backup data is a higher priority than the archive data. To prioritize both types of data, specify `BKREPLRULEDEFAULT=ACTIVE_DATA_HIGH_PRIORITY ARREPLRULEDEFAULT=ALL_DATA`.

You can specify the following rules:

ALL_DATA
: Replicates active and inactive backup data, archive data, or space-managed data. The data is replicated with a normal priority.

ACTIVE_DATA
: Replicates only active backup data. The data is replicated with a normal priority. This rule is valid only for BKREPLRULEDEFAULT.
Attention:

  If you specify ACTIVE_DATA and one or more of the following conditions are true, inactive backup data on the target replication server is deleted, and inactive backup data on the source replication server is not replicated.

  - When a release version earlier than Version 7.1.1 is installed on either the source or target replication servers.
  - When you are using the REPLICATE NODE command with the `FORCERECONCILE=YES` parameter.
  - When you are running the initial replication of a file space after you configure replication, restore the database, or upgrade both the source and target replication servers from a release version earlier than V7.1.1.

  If the previous conditions are not true, all new and changed files since the last replication are replicated, including inactive files, and files are deleted when they expire.

ALL_DATA_HIGH_PRIORITY
: Replicates active and inactive backup data, archive data, or space-managed data. Data is replicated with a high priority.

ACTIVE_DATA_HIGH_PRIORITY
: This rule is the same as the ACTIVE_DATA replication rule except data is replicated with a high priority. This rule is valid only for BKREPLRULEDEFAULT.

DEFAULT
: Replicates data according to the server replication rule for backup data.

  For example, suppose that you want to replicate the archive data in all the file spaces that belongs to a client node. Replication of the archive data is a high priority. One method to accomplish this task is to specify `ARREPLRULEDEFAULT=DEFAULT`. Ensure that the file space rules for archive data are also set to DEFAULT and that the server rule for archive data is set to ALL_DATA_HIGH_PRIORITY.

Restriction: If a node is configured for replication, the file space rules are set to DEFAULT after the node stores data on the source replication server.

NONE
: Data of the specified type is not replicated.

  For example, if you do not want to replicate space-managed data that belongs to a client node, specify `SPREPLRULEDEFAULT=NONE`

REPLState
: Specifies whether data that belongs to the client node is ready to be replicated. This parameter is optional. You can specify one of the following values:

  ENabled
  : Specifies that the client node is ready for replication.

  DISabled
  : Specifies that replication does not occur until you enable it.

  The system response to these settings depends on the following factors:

  Whether the client node definition exists only on the source replication server and you are configuring the client node for replication for the first time
  : If you set the replication state to ENABLED or DISABLED, the replication mode of the node on the source replication server is automatically set to SEND after the UPDATE NODE command is issued. When replication first occurs, a client node definition on the target server is automatically created. The replication state of the client node on the target server is automatically set to ENABLED. The replication mode is set to RECEIVE.

  Whether the client node definition exists on the source and the target replication servers, and the node data was previously replicated
  : For replication to occur, the replication state of the client node on both the source and the target servers must be set to ENABLED. For example, if the replication state of a client node on the source server is ENABLED and the replication state on the target server is DISABLED, replication does not occur.

  Whether the client node definition exists on the source and the target replication servers, and the node data was previously exported from the source replication server and imported to the target replication server
  : In this case, you are configuring the client nodes to synchronize the data between the two servers. When replication first occurs, the replication state of the client node on the target server is automatically set to ENABLED. Data on the source and target servers is synchronized.
    Restriction: To synchronize data, you must specify the REPLMODE parameter in addition to the REPLSTATE parameter.

  You can specify the REPLMODE parameter only if the client node has never been replicated:

  - If the client node definition exists only on the source replication server, the replication mode of the node on the source replication server is automatically set to SEND when the UPDATE NODE command is issued. The replication mode of the node on the target replication server is automatically set to RECEIVE.
  - If data that belongs to the node was previously replicated, the replication mode of the node on the source replication server is SEND. The replication mode of the node on the target replication server is RECEIVE.

REPLMode
: Specifies whether to synchronize the data that belongs to this client node. Specify this parameter only if data that belongs to the client node was exported from the source replication server and imported to the target replication server. Synchronization occurs during replication.

  To synchronize data, you must issue the UPDATE NODE command on both the source and target replication servers and specify the REPLMODE and REPLSTATE parameters. The value that you specify for the REPLMODE parameter depends on whether the server is a source of or a target for replicated data.

  You can specify one of the following values:

  SYNCSEnd
  : Specifies that data that belongs to this client node is synchronized with data on a target server during replication. Specify this value only on the server that exported the data. When the synchronization is complete, the replication mode for the client node on the source server is automatically set to SEND. The replication mode remains SEND unless you remove the node by issuing the REMOVE REPLNODE command.

  SYNCRECeive
  : Specifies that data that belongs to this client node is synchronized with data on a source server during replication. Specify this value only on the server that imported the data. When the synchronization is complete, the replication

mode for the client node on the target server is automatically set to RECEIVE. The replication mode remains RECEIVE unless you remove the node by issuing the REMOVE REPLNODE command.

Restrictions:

- You can set the REPLMODE parameter only if the initial replication state is NONE. To synchronize data, you change the replication state to ENABLED or DISABLED and specify a value for the REPLMODE parameter.
- Data can be synchronized only if you specified `DATES=ABSOLUTE` on the IMPORT NODE command. If you specified `DATES=RELATIVE` to import data, you must rename the node or delete its data before replication. If you do not take one of these steps, you can lose data.
- If the REPLMODE parameter was set incorrectly, you must issue the REMOVE REPLNODE command before you update the client node definition. For example, suppose that you updated the definition of a client node whose data you wanted to replicate. The data that belongs to the node was previously exported to the target replication server. You specified ENABLED as the setting of the REPLSTATE parameter. However, you did not specify SYNCSEND on the source replication server. As a result, the REPLMODE parameter was automatically set to SEND, and data that belongs to the node could not be synchronized or replicated.

  Issuing REMOVE REPLNODE sets the replication state and the replication mode to NONE. After the REMOVE REPLNODE command is completed, reissue the UPDATE NODE command with the correct parameters and values.

RECOVERDamaged
: Specifies whether damaged files can be recovered for this node from a target replication server. The parameter is optional. The default value is YES. You can specify one of the following values:

  Yes
  : Specifies that recovery of damaged files from a target replication server is enabled for this node.

  No
  : Specifies that recovery of damaged files from a target replication server is not enabled for this node.
  Tip: The value of the RECOVERDAMAGED parameter is only one of several settings that determine whether damaged files are recovered. For information about how to specify the settings, see Settings that affect the recovery of damaged files.

ROLEOVERRIDE

: Specifies whether to override the reported role of the client for processor value unit (PVU) estimation reporting. The default is USEREPORTED.

  The role reported by the client is either client-device (for example, a workstation) or server-device (for example, file/print server, application server, database). By default, the client reports its role that is based on the client type and the operating system. All clients initially report their role as server-device, except for IBM Spectrum Protect backup-archive clients that are running Microsoft Windows workstation distributions (Windows Vista) and Macintosh OS X.

  Specify one of the following values:

  Client
  : Specifies a client-device.

  Server
  : Specifies a server-device.

  Other
  : Specifies that this node is not to be used for PVU estimation reporting. The Other value is useful when multiple nodes are deployed for a physical system (for example, virtual environments, test nodes, retired nodes, and nodes not in production or clustering).

  Usereported
  : Use the reported role that is provided by the client.

AUTHentication
: This parameter determines the password authentication method that you use; either LDAP or LOCAL.

  LOcal
  : Specifies that the node uses the local IBM Spectrum Protect server database to store passwords.

  LDap
  : Specifies that the node uses an LDAP directory server to authenticate passwords. Passwords are not stored in the IBM Spectrum Protect database.

SYNCldapdelete

This parameter applies only if you want a node that authenticates with a Lightweight Directory Access Protocol (LDAP) server to change to authenticate with the IBM Spectrum Protect server. The parameter specifies whether to remove the node from the LDAP server.

Yes
: Specifies that the node is removed.
Restriction: Do not specify a value of YES. (The value of YES is appropriate only for users of the previous LDAP authentication method, which is described in Managing passwords and logon procedures.)

No
: Specifies that the node is not removed. This is the default value.

SSLrequired (deprecated)

Specifies whether the node must use the Secure Sockets Layer (SSL) protocol to communicate with the IBM Spectrum Protect server. The parameter is optional. When you authenticate passwords with an LDAP directory server, you must protect the sessions by using SSL or another network security method.

Important: Beginning with IBM Spectrum Protect V8.1.2 software and Tivoli Storage Manager V7.1.8 software, this parameter is deprecated. The validation that was enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The SSLREQUIRED parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

SESSIONSECurity
: Specifies whether the node must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

You can specify one of the following values:

STRict
: Specifies that the strictest security settings are enforced for the node. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the server and the node. To specify whether the server uses TLS 1.2 for the entire session or only for authentication, see the SSL client option.
To use the STRICT value, the following requirements must be met to ensure that the node can authenticate with the server:

- Both the node and server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
- The node must be configured to use the TLS 1.2 protocol for SSL sessions between the server and the node.

Nodes set to STRICT that do not meet these requirements are unable to authenticate with the server.

TRANSitional
: Specifies that the existing security settings are enforced for the node. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the node has never met the requirements for the STRICT value, the node will continue to authenticate by using the TRANSITIONAL value. However, after a node meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the node can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after a node successfully authenticates by using a more secure communication protocol, the node can no longer authenticate by using a less secure protocol. For example, if a node that is not using SSL is updated and successfully authenticates by using TLS 1.2, the node can no longer authenticate by using no SSL protocol or by using TLS 1.1. This restriction also applies when you use functions such as virtual volumes, when the node authenticates to the IBM Spectrum Protect server as a node from another server.

SPLITLARGEObjects
: Specifies whether large objects that are stored by this node are automatically split into smaller pieces, by the server, to optimize server processing. Specifying Yes causes the server to split large objects (over 10 GB) into smaller pieces when stored by a client node. Specifying No bypasses this process. Specify No only if your primary concern is maximizing throughput of backups directly to tape. The default value is Yes.

Example: Update node SIMON to authenticate with an LDAP directory server and connect using SSL

```
update node simon authentication=ldap sslrequired=yes
```

When you specify the SSLREQUIRED parameter, the server is not automatically configured for SSL. You must follow the instructions for connecting with SSL in order for the example to work.

Example: Update all nodes to communicate with a server by using strict session security

Update all nodes to use the strictest security settings to authenticate with the server.

```
update node * sessionsecurity=strict
```

Example: Update a node with software release information for a future deployment

The client deployment feature helps you update a backup-archive client to a newer release. The information that is generated from the UPDATE NODE command can help you when you plan a deployment. The information is stored for a future deployment and can be viewed by issuing the QUERY NODE command. After a deployment, you can issue the QUERY NODE command to see the current level and the target level. For example, to update node LARRY to backup-archive client Version 6.3.0.0.

```
update node LARRY targetlevel=6.3.0.0
```

Example: Update a node backup to compress data and keep the client from deleting archived files

Update node LARRY so that the data on node LARRY is compressed when it is backed up or archived by IBM Spectrum Protect and so that the client cannot delete archived files.

```
update node larry compression=yes archdelete=no
```

Example: Update a node's number of files that can be transferred as a group

Update node LARRY and increase the TXNGroupmax value to 1,000.

```
update node larry txngroupmax=1000
```

Example: Update a node and allow it to deduplicate on the client

Update a node BOB so that it can deduplicate on the client.

```
update node bob deduplication=clientorserver
```

Example: Update the role of node BOB to a server-device for PVU estimation reporting

If you want to accumulate PVU values, only server device roles are recorded. You can update a node from client-device to server-device by issuing the UPDATE NODE command. For this example, node BOB is updated to a server-device.

```
update node bob role=server
```

Example: Update a node definition on a source replication server

NODE1 is defined to a source replication server. The data that belongs to NODE1 was previously exported to a target replication server. Update the replication rule for backup data that belongs to NODE1 so that active backup data is replicated with a high priority. Enable replication for the node. Set up data synchronization with the target replication server.

```
update node node1 bkreplruledefault=active_data_high_priority
replstate=enabled replmode=syncsend
```

Example: Update a node definition to enable recovery of damaged files

Update the PAYROLL node to enable the recovery of damaged files from a target replication server.

```
update node payroll recoverdamaged=yes
```

Related commands

Table 2. Commands related to UPDATE NODE

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY PVUESTIMATE	Displays an estimate of the client-devices and server-devices being managed.
QUERY REPLNODE	Displays information about the replication status of a client node.
REGISTER ADMIN	Defines a new administrator without granting administrative authority.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
REMOVE REPLNODE	Removes a node from replication.
RENAME NODE	Changes the name for a client node.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
RESET PASSEXP	Resets the password expiration for nodes or administrators.
SET DEDUPVERIFICATIONLEVEL	Specifies the percentage of extents verified by the server during client-side deduplication.
SET PASSEXP	Specifies the number of days after which a password is expired and must be changed.
SET REPLRECOVERDAMAGED	Specifies whether node replication is enabled to recover damaged files from a target replication server.
UPDATE ADMIN	Changes the password or contact information associated with any administrator.
UPDATE FILESPACE	Changes file-space node-replication rules.

Related reference:
Ssl client option

UPDATE NODEGROUP (Update a node group)

Use this command to modify the description of a node group.

Privilege class

To issue this command, you must have system or unrestricted policy privilege.

Syntax

```
>>-UPDate NODEGroup--group_name--DESCription--=--description--->< 
```

Parameters

group_name
: Specifies the name of the node group whose description you want to update.

DESCription (Required)
: Specifies a description of the node group. This parameter is required. The maximum length of the description is 255 characters. If the description contains any blanks, enclose the entire description in quotation marks.

Example: Update a node group's description

Update the node group, `group1`, with a new description.

```
update nodegroup group1 description="Human Resources"
```

Related commands

Table 1. Commands related to UPDATE NODEGROUP

Command	Description
DEFINE BACKUPSET	Defines a previously generated backup set to a server.
DEFINE NODEGROUP	Defines a group of nodes.
DEFINE NODEGROUPMEMBER	Adds a client node to a node group.
DELETE BACKUPSET	Deletes a backup set.
DELETE NODEGROUP	Deletes a node group.
DELETE NODEGROUPMEMBER	Deletes a client node from a node group.
GENERATE BACKUPSET	Generates a backup set of a client's data.
QUERY BACKUPSET	Displays backup sets.
QUERY NODEGROUP	Displays information about node groups.
UPDATE BACKUPSET	Updates a retention value associated with a backup set.

UPDATE PATH (Change a path)

Use this command to update a path definition.

Syntax and parameter descriptions are available for the following path types.

- UPDATE PATH (Change a path when the destination is a drive)
- UPDATE PATH (Change a path when the destination is a library)
- AIX Linux UPDATE PATH (Update a path when the destination is a ZOSMEDIA library)

For detailed and current device support information, see the Supported Devices website for your operating system:

- AIX Windows Supported devices for AIX and Windows
- Linux Supported devices for Linux

Related commands

Table 1. Commands related to UPDATE PATH

Command	Description
DEFINE DATAMOVER	Defines a data mover to the IBM Spectrum Protect server.
DEFINE DRIVE	Assigns a drive to a library.
DEFINE LIBRARY	Defines an automated or manual library.
DEFINE PATH	Defines a path from a source to a destination.
DELETE PATH	Deletes a path from a source to a destination.
QUERY PATH	Displays information about the path from a source to a destination.
UPDATE DATAMOVER	Changes the definition for a data mover.

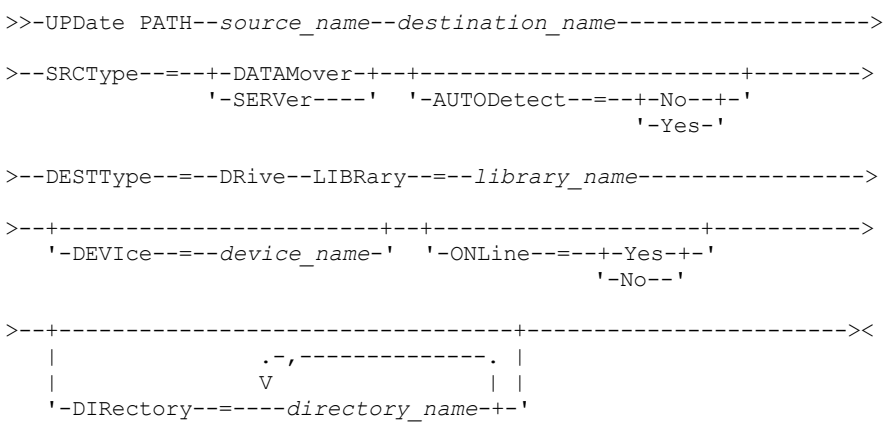
UPDATE PATH (Change a path when the destination is a drive)

Use this syntax when updating a path definition to a drive.

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax



Parameters

source_name (Required)
: Specifies the name of source for the path. This parameter is required.

destination_name (Required)
: Specifies the name of the destination. This parameter is required.

SRCType (Required)
: Specifies the type of the source. This parameter is required. Possible values are:

  DATAMover
  : Specifies that a data mover is the source.

  SERVer
  : Specifies that a server or a storage agent is the source.

AUTODetect
: Specifies whether the serial number for a drive or library will be automatically detected, reported, and updated in IBM Spectrum Protect™. This parameter is optional. This parameter is only valid for paths defined from the local server to a drive or a library. Possible values are:

  No
  : Specifies that the serial number is not automatically updated.

  Yes
  : Specifies that the serial number is automatically updated to reflect the same serial number that the drive reports to IBM Spectrum Protect.
  Important:

  1. If you have not previously entered a serial number, then AUTODETECT defaults to YES. If you have previously entered a serial number, then AUTODETECT defaults to NO.
  2. AUTODETECT=YES in this command overrides the serial number set in the DEFINE DRIVE command.
  3. If you set DESTTYPE=DRIVE and AUTODETECT=YES, then the drive element number in the IBM Spectrum Protect database will be automatically changed to reflect the same element number that corresponds to the serial number of that drive. This is true for drives in a SCSI library. For more information about the element number, see the DEFINE DRIVE command.
  4. Depending on the capabilities of the device, the AUTODETECT parameter may not be supported.

DESTType=DRive (Required)
: Specifies that a drive is the destination. When the destination is a drive, you must specify a library name. This parameter is required.

LIBRary

Specifies the name of the library to which the drive is assigned. The library and its drives must already be defined to the server. If the path is from a NAS data mover to a library, the library must have LIBTYPE of SCSI, 349x, or ACSLS.

DEVIce

Specifies the name of the device as known to the source, or FILE if the device is a logical drive in a FILE library.

AIX The source uses the device name to access the drive. See Table 1 for examples.

Table 1. Examples of device names

Source to destination	Example
Server to a drive (not a FILE drive)	AIX `/dev/rmt3`
Storage agent to a drive (not a FILE drive)	`mt3`
Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`
NAS data mover to a drive	NetApp NAS file server: `rst01` EMC Celerra NAS file server: `c436t011` IBM® System Storage® N Series: `rst01`

Linux The source uses the device name to access the drive. See Table 2 for examples.

Table 2. Examples of device names

Source to destination	Example
Server to a drive (not a FILE drive)	`/dev/tsmscsi/mt3`
Storage agent to a drive (not a FILE drive)	`/dev/tsmscsi/mt3`
Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`
NAS data mover to a drive	NetApp NAS file server: `rst01` EMC Celerra NAS file server: `c436t011` IBM System Storage N Series: `rst01`

Windows The source uses the device name to access the drive. See Table 3 for examples.

Table 3. Examples of device names

Source to destination	Example
Server to a drive (not a FILE drive)	Windows `mt3`
Server to a drive (REMOVABLEFILE drive)	`e:`
Storage agent to a drive (not a FILE drive)	`mt3`
Storage agent to a drive when the drive is a logical drive in a FILE library	`FILE`
NAS data mover to a drive	NetApp NAS file server: `rst01` EMC Celerra NAS file server: `c436t011` IBM System Storage N Series: `rst01`

Important:

- For 349X libraries, the alias name is a symbolic name that is specified in the /etc/ibmatl.conf file. For more information, see *IBM Tape Device Drivers Installation and User's Guide*, which can be downloaded from the IBM Systems support site at http://www.ibm.com/support/docview.wss?uid=ssg1S7002972.
- For information about how to obtain names for devices that are connected to a NAS file server, consult the product information for the file server. For example, for a NetApp file server, connect to the file server using Telnet and issue the SYSCONFIG command. Use this command to determine device names for drives:

  ```
  sysconfig -t
  ```

ONLine

Specifies whether the path is available for use. This parameter is optional. Possible values are:

Yes
: Specifies that the path is available for use.

No
: Specifies that the path is not available for use.

The source and the destination must both be available to use the path.

For example, if the path from a data mover to a drive is online, but either the data mover or the drive is offline, you cannot use the path.

DIRectory

Specifies the directory location or locations for a storage agent to access the files in a FILE library. The DIRECTORY parameter is also used for devices of type REMOVABLEFILE. For REMOVABLEFILE devices, the DIRECTORY parameter provides information for the server (not a storage agent) along with the DRIVE parameter to describe access to the device. This parameter is optional.
On storage agents, this parameter is only valid when *all* of the following conditions are true:

- The source type is SERVER (meaning a storage agent that has been defined as a server to this server).
- The source name is the name of a storage agent, *not* the server.
- The destination is a logical drive that is part of a FILE library.
- If multiple directories were specified for the device class associated with the FILE library, the same number of directories must be specified with the DIRectory parameter of the DEFINE PATH command, for each drive in the FILE library. Storage agent directories are not validated on the server. Specifying incorrect directories can cause a run-time failure.

The directory name or names identify the locations where the storage agent reads and writes the files that represent storage volumes for the FILE device class that is associated with the FILE library. The default value for DIRECTORY is the directory of the server at the time the command is issued.

Use a naming convention that you can use to associate the directory with a particular physical drive. This can help ensure that your configuration is valid for sharing the FILE library between the server and storage agent. If the storage agent is on a Windows system, use a universal naming convention (UNC) name. When the storage agent lacks permission to access remote storage, the storage agent will experience mount failures.

Windows The account associated with the storage agent service must be either an account within the local administrator's group or an account within the domain administrator's group. If the account is in the local administrator's group, the user ID and password must match that of an account with permissions to access storage as provided by the machine which administers the remote share. For example, if a SAMBA server is providing access to remote storage, the user ID and password in the SAMBA configuration must match that of the local administrator user ID and password associated with the storage agent service.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path sta1 file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```

In the previous example, the DEFINE DEVCLASS command establishes the shared file system in the directory accessed by the server as D:\FILEDIR\DIR1. The storage agent, however, is using UNC name \\192.168.1.10\FILEDIR\DIR1. This means that the machine with TCP/IP address 192.168.1.10 is sharing the same directory using FILEDIR as the shared name. Also, the storage agent service has an account which can access this storage. It can access it either because it is associated with a local account with the same user ID and password as 192.168.1.10 or it is associated with a domain account which is available on both the storage agent and on 192.168.1.10. If appropriate to the installation, you can replace the 192.168.1.10 with a symbolic name such as:

```
example.yourcompany.com
```

Important:

- IBM Spectrum Protect does not create shares or permissions, or mount the target file system. You must perform these actions before starting the storage agent.
- You can modify a list of directories only by replacing the entire list.
- You must ensure that storage agents can access newly created FILE volumes. To access FILE volumes, storage agents replace names from the directory list in the device-class definition with the names in the directory list for the associated path definition. The following illustrates the importance of matching device classes and paths to ensure that storage agents can access newly created FILE volumes.
  Suppose you want to use these three directories for a FILE library: Windows
  - c:\server
  - d:\server
  - e:\server

  AIX Linux
  - /opt/tivoli1

- /opt/tivoli2
- /opt/tivoli3

1. You use the following command to set up a FILE library named CLASSA with one drive named *CLASSA1* on *SERVER1*: Windows

   ```
   define devclass classa devtype=file
   directory="c:\server,d:\server,e:\server"
   shared=yes mountlimit=1
   ```

   AIX Linux

   ```
   define devclass classa devtype=file
   directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
   shared=yes mountlimit=1
   ```

2. You want the storage agent `STA1` to be able to use the FILE library, so you define the following path for storage agent `STA1`: Windows

   ```
   define path server1 sta1 srctype=server desttype=drive device=file
   directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
   \\192.168.1.10\e\server" library=classa
   ```

   Windows In this scenario, the storage agent, `STA1`, will replace the directory name c:\server with the directory name \\192.168.1.10\c\server to access FILE volumes that are in the c:\server directory on the server.

   AIX Linux

   ```
   define path server1 sta1 srctype=server desttype=drive device=file
   directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
   ```

   AIX Linux In this scenario, the storage agent, `STA1`, will replace the directory name /opt/tivoli1 with the directory name /opt/ibm1/ to access FILE volumes that are in the /opt/tivoli1 directory on the server.

3. Windows File volume c:\server\file1.dsm is created by SERVER1. If you later change the first directory for the device class with the following command:

   ```
   update devclass classa directory="c:\otherdir,d:\server,e:\server"
   ```

   SERVER1 will still be able to access file volume c:\server\file1.dsm, but the storage agent `STA1` will not be able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume will still be accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.

4. AIX Linux If file volume /opt/tivoli1/file1.dsm is created on *SERVER1*, and if the following command is issued,

   ```
   update devclass classa directory="/opt/otherdir,/opt/tivoli2,
   /opt/tivoli3"
   ```

   SERVER1 will still be able to access file volume /opt/tivoli1/file1.dsm, but the storage agent `STA1` will not be able to access it because a matching directory name in the PATH directory list no longer exists. If a directory name is not available in the directory list associated with the device class, the storage agent can lose access to a FILE volume in that directory. Although the volume will still be accessible from the server for reading, failure of the storage agent to access the FILE volume can cause operations to be retried on a LAN-only path or to fail.

Example: Update a path from a data mover NAS file server to a tape drive

Update a path from a data mover that is a NAS file server to the drive *TAPEDRV2* that the data mover uses for backup and restore operations. In this example, the NAS data mover is *NAS1*, the library is *NASLIB*, and the device name for the drive is *rst0l*.

```
update path nas1 tapedrv2 srctype=datamover desttype=drive library=naslib
    device=rst0l
```

UPDATE PATH (Change a path when the destination is a library)

Use this syntax when updating a path definition to a library.

Privilege class

To issue this command you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate PATH--source_name--destination_name------------------>

>--SRCType--=--+-DATAMover-+--+-----------------------+-------->
               '-SERVer----'  '-AUTODetect--=--+-No--+-'
                                               '-Yes-'

>--DESTType--=--LIBRary--+-------------------------------+------>
                         +-DEVIce--=--device_name--------+
                         '-EXTERNALManager--=--path_name-'

>--+--------------------+---------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Parameters

source_name (Required)
: Specifies the name of source for the path. This parameter is required.

destination_name (Required)
: Specifies the name of the destination. This parameter is required.
Important: To define a path from a NAS data mover to a library, the library must have LIBTYPE of SCSI, 349X, or Automated Cartridge System Library Software (ACSLS).

SRCType (Required)
: Specifies the type of the source. This parameter is required. Possible values are:

  DATAMover
  : Specifies that a data mover is the source.

  SERVer
  : Specifies that a server or a storage agent is the source.

AUTODetect
: Specifies whether the serial number for a drive or library is automatically detected, reported, and updated in IBM Spectrum Protect™. This parameter is optional. This parameter is only valid for paths defined from the local server to a library.
Possible values are:

  No
  : Specifies that the serial number is not automatically updated.

  Yes
  : Specifies that the serial number is automatically updated to reflect the same serial number that the drive reports to IBM Spectrum Protect.
  Important:

    1. If you have not previously entered a serial number, then AUTODETECT defaults to YES. If you have previously entered a serial number, then AUTODETECT defaults to NO.
    2. AUTODETECT=YES in this command overrides the serial number set in the DEFINE DRIVE command.
    3. Depending on the capabilities of the device, the AUTODETECT parameter may not be supported.

DESTType=LIBRary (Required)
: Specifies that a library is the destination.. This parameter is required.

DEVIce
: Specifies the name of the device as known to the source, or FILE if the device is a logical drive in a FILE library.
AIX The source uses the device name to access the drive or library. See Table 1 for examples.

Table 1. Examples of device names

Source to destination	Example

Source to destination	Example
Server to a library	AIX /dev/lb4 Linux /dev/tsmscsi/lb4
NAS data mover to a library	mc0

Linux The source uses the device name to access the drive or library. See Table 2 for examples.

Table 2. Examples of device names

Source to destination	Example
Server to a library	/dev/tsmscsi/lb4
NAS data mover to a library	mc0

Windows The source uses the device name to access the drive or library. See Table 3 for examples.

Table 3. Examples of device names

Source to destination	Example
Server to a library	Windows lb4.1
NAS data mover to a library	mc0

Important:

- For 349X libraries, the alias name is a symbolic name that is specified in the /etc/ibmatl.conf file. For more information, see *IBM Tape Device Drivers Installation and User's Guide*, which can be downloaded from the IBM® Systems support site at http://www.ibm.com/support/docview.wss?uid=ssg1S7002972.
- For information about how to obtain names for devices that are connected to a NAS file server, consult the product information for the file server. For example, for a NetApp file server, connect to the file server using Telnet and issue the SYSCONFIG command. Use this command to determine the device name for a library:

  ```
  sysconfig -m
  ```

EXTERNALManager

Specifies the location of the external library manager where IBM Spectrum Protect can send media access requests. Use single quotation marks around the value of this parameter. For example, enter: AIX

```
/usr/lpp/GESedt-acsls/bin/elmdt
```

Linux

```
/opt/GESedt-acsls/bin/elmdt
```

Windows

```
C:\Program Files\GES\EDT-ACSLS\bin\elmdt.exe
```

This parameter is required when the library name is an external library.

ONLine

Specifies whether the path is available for use. This parameter is optional. Possible values are:

Yes
: Specifies that the path is available for use.

No
: Specifies that the path is not available for use.

The source and the destination must both be available to use the path.

Important: If the path to a library is offline, the server will not be able to access the library. If the server is halted and restarted while the path to the library is offline, the library will not be initialized.

AIX Linux

UPDATE PATH (Update a path when the destination is a ZOSMEDIA library)

Use this syntax when you update a path to a ZOSMEDIA library.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate PATH--source_name--destination_name------------------>

>--SRCType--=--SERVer--DESTType--=--LIBRary--------------------->

>--ZOSMEDIASERVER--=--server_name--+--------------------+------><
                                   '-ONLine--=--+-Yes-+-'
                                                '-No--'
```

Parameters

source_name (Required)
: Specifies the name of source for the path.

destination_name (Required)
: Specifies the name of the destination.

SRCType=SERVer (Required)
: Specifies that the IBM Spectrum Protect™ server or a storage agent is the source.

DESTType=LIBRary (Required)
: Specifies that a library is the destination.

ZOSMEDIAServer (Required)
: Specifies the server name that represents a Tivoli® Storage Manager for z/OS® Media server.

ONLine
: Specifies whether the path is available for use. This parameter is optional. Possible values are:

  Yes
  : Specifies that the path is available for use.

  No
  : Specifies that the path is not available for use.

  The source and the destination must both be available to use the path.

  Important: If the path to a library is offline, the server cannot access the library. If the server is halted and restarted while the path to the library is offline, the library is not initialized during server initialization. The path must be updated to ONLINE=YES to access the library.

UPDATE POLICYSET (Update a policy set description)

Use this command to change the description of a policy set. You cannot change the description of the ACTIVE policy set.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-UPDate POlicyset--domain_name--policy_set_name--------------->

>--DESCription--=--description--------------------------------><
```

Parameters

domain_name (Required)
: Specifies the policy domain to which the policy set belongs.

policy_set_name (Required)
Specifies the policy set to update. You cannot change the ACTIVE policy set.
DESCription (Required)
Specifies text that describes the policy set. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove a previously defined description, specify a null string ("").

Example: Update a policy set

Update a policy set called `VACATION` for the `EMPLOYEE_RECORDS` policy domain with a description of "Schedule Planning Information."

```
update policyset employee_records vacation
description="schedule planning information"
```

Related commands

Table 1. Commands related to UPDATE POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY MGMTCLASS	Creates a copy of a management class.
DEFINE DOMAIN	Defines a policy domain that clients can be assigned to.
DEFINE MGMTCLASS	Defines a management class.
DEFINE POLICYSET	Defines a policy set within the specified policy domain.
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY POLICYSET	Displays information about policy sets.
VALIDATE POLICYSET	Verifies and reports on conditions the administrator must consider before activating the policy set.

UPDATE PROFILE (Update a profile description)

Use this command on a configuration manager to update a profile description.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UPDate PROFIle--profile_name--DESCription-=--description--->< 
```

Parameters

profile_name (Required)
Specifies the profile to update.
DESCription (Required)
Specifies a description for the profile. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove a description, specify a null string ("").

Example: Update a profile's description

Update the description for profile DELTA.

```
update profile delta description="PAYROLL domain"
```

Related commands

Table 1. Commands related to UPDATE PROFILE

Command	Description
COPY PROFILE	Creates a copy of a profile.
DEFINE PROFASSOCIATION	Associates objects with a profile.
DEFINE PROFILE	Defines a profile for distributing information to managed servers.
DELETE PROFASSOCIATION	Deletes the association of an object with a profile.
DELETE PROFILE	Deletes a profile from a configuration manager.
LOCK PROFILE	Prevents distribution of a configuration profile.
QUERY PROFILE	Displays information about configuration profiles.
SET CONFIGMANAGER	Specifies whether a server is a configuration manager.
UNLOCK PROFILE	Enables a locked profile to be distributed to managed servers.

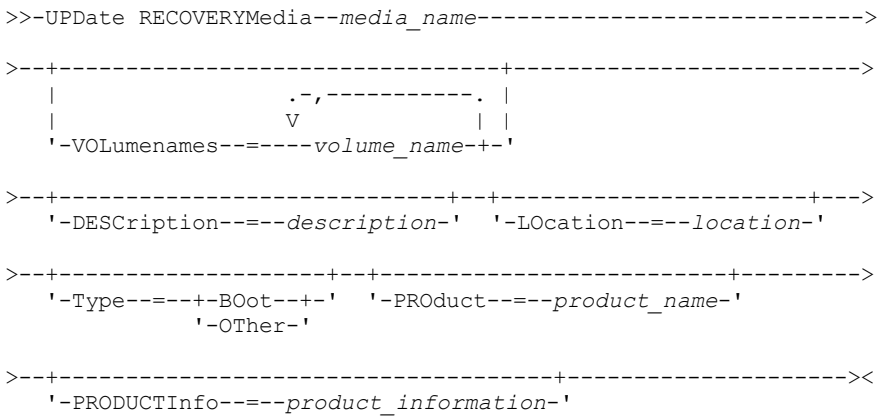
UPDATE RECOVERYMEDIA (Update recovery media)

Use this command to update information about recovery media.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

media_name (Required)
: Specifies the name of the recovery media to be updated.

VOLumenames
: Specifies the names of volumes that contain the recoverable data (for example, operating system image copies). If you specify a TYPE=BOOT, you must specify the boot media volume names in the order in which they are to be loaded at recovery time. The volume names list can be up to 255 characters. Enclose the list in quotation marks if it contains any blank characters. To remove all volume names, specify a null string ("").

DESCription
: Specifies the description of the recovery media. This parameter is optional. You can use up to 255 characters. Enclose the text in quotation marks if it contains any blank characters.

LOcation

Describes the location of the recovery media. This parameter is optional. You can use up to 255 characters. Enclose the text in quotation marks if it contains any blank characters. To remove a location description, specify a null string ("") for the value.

Type

Specifies the type of recovery media. This parameter is optional. Possible values are:

BOot

Specifies that this is boot media. You must specify volume names if the type is BOOT.

OTher

Specifies that this is not boot media. For example, a CD that contains operating system manuals.

PROduct

Specifies the name of the product that wrote to this media. This parameter is optional. You can use up to 16 characters. Enclose the text in quotation marks if it contains any blank characters. To remove a product name, specify a null string ("") for the value.

PRODUCTInfo

Specifies any information about the product that wrote to the media that you may need to restore the machine. This parameter is optional. You can use up to 255 characters. Enclose the text in quotation marks if it contains any blank characters. To remove previously defined product information, specify a null string ("") for the value.

Example: Update a recovery media's location description

Update the location description for recovery media DIST5RM to "Corporate Headquarters Data Vault."

```
update recoverymedia dist5rm
location="Corporate Headquarters Data Vault"
```

Related commands

Table 1. Commands related to UPDATE RECOVERYMEDIA

Command	Description
DEFINE RECOVERYMEDIA	Defines the media required to recover a machine.
DELETE RECOVERYMEDIA	Deletes recovery media.
QUERY RECOVERYMEDIA	Displays media available for machine recovery.

UPDATE REPLRULE (Update replication rules)

Use this command to enable or disable a replication rule.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UPDate REPLRule--rule_name----STate--=--+-ENabled--+--------><
                                            '-DISabled-'
```

Parameters

rule_name (Required)

Specifies the name of the replication rule to be updated. You can use wildcard characters to specify one or more rules. You can specify one of the following rules:

- ALL_DATA
- ACTIVE_DATA

- ALL_DATA_HIGH_PRIORITY
- ACTIVE_DATA_HIGH_PRIORITY

STate (Required)
Specifies whether replication is allowed for the rule. You can specify one of the following values:

ENabled
Specifies that the data to which the rule applies is ready to be replicated
DISabled
Specifies that replication does not occur until you enable it.

Example: Disable replication for backup data

Disable replication of normal-priority, active-backup data for all file spaces in all client nodes that are configured for replication:

```
update replrule active_data state=disabled
```

Related commands

Table 1. Commands related to UPDATE REPLRULE

Command	Description
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLICATION	Displays information about node replication processes.
QUERY REPLRULE	Displays information about node replication rules.
SET ARREPLRULEDEFAULT	Specifies the server node-replication rule for archive data.
SET BKREPLRULEDEFAULT	Specifies the server node-replication rule for backup data.
SET SPREPLRULEDEFAULT	Specifies the server node-replication rule for space-managed data.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE NODE	Changes the attributes that are associated with a client node.
VALIDATE REPLICATION	Verifies replication for file spaces and data types.

UPDATE SCHEDULE (Update a schedule)

Use this command to update a client or administrative command schedule.

The UPDATE SCHEDULE command takes two forms, depending on whether the schedule applies to client operations or administrative commands. Within these two forms, you can select either classic or enhanced style schedules. The syntax and parameters for each form are defined separately.

Table 1. Commands related to UPDATE SCHEDULE

Command	Description
COPY SCHEDULE	Creates a copy of a schedule.
DEFINE SCHEDULE	Defines a schedule for a client operation or an administrative command.
DELETE SCHEDULE	Deletes a schedule from the database.
QUERY EVENT	Displays information about scheduled and completed events for selected clients.
QUERY SCHEDULE	Displays information about schedules.

Command	Description
SET MAXCMDRETRIES	Specifies the maximum number of retries after a failed attempt to execute a scheduled command.
SET MAXSCHEDSESSIONS	Specifies the maximum number of client/server sessions available for processing scheduled work.
SET RETRYPERIOD	Specifies the time between retry attempts by the client scheduler.

- UPDATE SCHEDULE (Update a client schedule)
  Use the UPDATE SCHEDULE to update selected parameters for a client schedule.
- UPDATE SCHEDULE (Update an administrative schedule)
  Use this command to update selected parameters for an administrative command schedule.

UPDATE SCHEDULE (Update a client schedule)

Use the UPDATE SCHEDULE to update selected parameters for a client schedule.

This command does not change the client associations that have been made to this schedule. Any clients that are associated with the original schedule, process the modified schedule.

Not all clients can run all scheduled operations, even though you can define the schedule on the server and associate it with the client. For example, a Macintosh client cannot run a schedule when the action is to restore or retrieve files, or run an executable script. An executable script is also known as a command file, a batch file, or a script on different client operating systems.

Privilege class

To update a client schedule, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the schedule belongs.

Syntax for a classic client schedule

```
                    (1)
>>-UPDate SCHedule--------domain_name--schedule_name------------>

>--+-----------------+--+-----------------------------+--------->
   '-Type--=--Client-'  '-DESCription--=--description-'

>--+-------------------------------------------------------------+-->
   '-ACTion--=--+-Incremental--------------------------------+-'
                +-Selective-----------------------------------+
                +-Archive--+-----------------------------+---+
                |          |               .-""-------. |   |
                |          '-SUBACTion--=--+----------+-'   |
                |                          '-FASTBack-'     |
                +-Backup--+-----------------------------+-+ |
                |         |               .-""----------. | |
                |         '-SUBACTion--=--+-------------+-' |
                |                         +-FASTBack----+   |
                |                         +-SYSTEMSTate-+   |
                |                         '-VM----------'   |
                +-REStore-------------------------------------+
                +-RETrieve------------------------------------+
                +-IMAGEBACkup---------------------------------+
                +-IMAGEREStore--------------------------------+
                +-Command-------------------------------------+
                +-Macro---------------------------------------+
                '-Deploy--------------------------------------'

>--+---------------------------+-------------------------------->
   '-OPTions--=--option_string-'

>--+---------------------------+--+--------------------+------->
   '-OBJects--=--object_string-'  '-PRIority--=--number-'
```

```
>--+--------------------+--+--------------------+--------------->
   '-STARTDate--=--date-'  '-STARTTime--=--time-'

>--+---------------------+--+---------------------------+------->
   '-DURation--=--number-'  '-DURUnits--=--+-Minutes----+-'
                                           +-Hours------+
                                           +-Days-------+
                                           '-INDefinite-'

>--+----------------------+--+-----------------------+---------->
   '-MAXRUNtime--=--number-'  '-SCHEDStyle--=--Classic-'

>--+--------------------+--+-------------------------+---------->
   '-PERiod--=--number-'  '-PERUnits--=--+-Hours---+-'
                                         +-Days----+
                                         +-Weeks---+
                                         +-Months--+
                                         +-Years---+
                                         '-Onetime-'

>--+-----------------------------+----------------------------->
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+--------------------------+------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-date--'
```

Notes:

1. You must specify at least one optional parameter on this command.

Syntax for an enhanced client schedule

```
                     (1)
>>-UPDate SCHedule--------domain_name--schedule_name------------>

>--+-----------------+--+----------------------------+--------->
   '-Type--=--Client-'  '-DESCription--=--description-'

>--+-------------------------------------------------------------+-->
   '-ACTion--=--+-Incremental-------------------------------+-'
                +-Selective-----------------------------------+
                +-Archive--+-------------------------------+---+
                |          '-SUBACTion--=--+-""--------+-'   |
                |                          '-FASTBack-'     |
                +-Backup--+-------------------------------+-+
                |         '-SUBACTion--=--+-""-----------+-' |
                |                         +-FASTBack-----+   |
                |                         +-SYSTEMSTate-+   |
                |                         +-VApp---------+   |
                |                         '-VM-----------'   |
                +-REStore-------------------------------------+
                +-RETrieve------------------------------------+
                +-IMAGEBACkup---------------------------------+
                +-IMAGEREStore--------------------------------+
                +-Command-------------------------------------+
                '-Macro-----------------------------------------'

>--+---------------------------+------------------------------->
   '-OPTions--=--option_string-'

>--+---------------------------+--+--------------------+------->
```

```
   '-OBJects--=--object_string-'  '-PRIority--=--number-'

>--+--------------------+--+--------------------+--------------->
   '-STARTDate--=--date-'  '-STARTTime--=--time-'

>--+---------------------+--+-------------------------+-------->
   '-DURation--=--number-'  '-DURUnits--=--+-Minutes-+-'
                                           +-Hours---+
                                           '-Days----'

>--+----------------------+--+------------------------+------->
   '-MAXRUNtime--=--number-'  '-SCHEDStyle--=--Enhanced-'

>--+-------------------------+--+-----------------------+------>
   '-MONth--=--+-ANY-------+-'  '-DAYOFMonth--=--+-ANY-+-'
               +-JAnuary---+                    '-Day-'
               +-February--+
               +-MARch-----+
               +-APril-----+
               +-May-------+
               +-JUNe------+
               +-JULy------+
               +-AUgust----+
               +-September-+
               +-October---+
               +-November--+
               '-December--'

>--+---------------------------+------------------------------->
   '-WEEKofmonth--=--+-ANY----+-'
                     +-FIrst--+
                     +-Second-+
                     +-Third--+
                     +-FOurth-+
                     '-Last---'

>--+----------------------------+------------------------------->
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+-------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-date--'
```

Notes:

1. You must specify at least one optional parameter on this command.

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which this schedule belongs.

schedule_name (Required)
: Specifies the name of the schedule to be updated.

Type=Client
: Specifies that a client schedule is updated. This parameter is optional. The default is CLIENT.

DESCription
: Specifies a description of the schedule. This parameter is optional. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains blank characters. To remove a previously defined description, specify a null string ("") for this value.

ACTion
: Specifies the action that occurs when this schedule is processed. Possible values are:

Incremental
: Specifies that the schedule backs up all files that are new or that have changed since the last incremental backup. Incremental also backs up any file for which all existing backups might have expired.

Selective
: Specifies that the schedule backs up only files that are specified with the OBJECTS parameter.

Archive
: Specifies that the schedule archives files that are specified with the OBJECTS parameter.

Backup
: Specifies that the schedule backs up files that are specified with the OBJECTS parameter.

REStore
: Specifies that the schedule restores files that are specified with the OBJECTS parameter.

  When you specify ACTION=RESTORE for a scheduled operation, and the REPLACE option is set to PROMPT, no prompting occurs. If you set the option to PROMPT, the files are skipped.

  If you specify a second file specification, this second file specification acts as the restore destination. If you need to restore multiple groups of files, schedule one for each file specification that you need to restore.

RETrieve
: Indicates that the schedule retrieves files that are specified with the OBJECTS parameter.
  Remember: A second file that is specified acts as the retrieve destination. If you need to retrieve multiple groups of files, create a separate schedule for each group of files.

IMAGEBACkup
: Specifies that the schedule backs up logical volumes that are specified with the OBJECTS parameter.

IMAGEREStore
: Specifies that the schedule restores logical volumes that are specified with the OBJECTS parameter.

Command
: Specifies that the schedule processes a client operating system command or script that is specified with the OBJECTS parameter.

Macro
: Specifies that a client processes a macro whose file name is specified with the OBJECTS parameter.

SUBACTion
: You can specify one of the following values:

  ""
  : When a null string (two double quotes) is specified with ACTION=BACKUP the backup is an incremental.

  FASTBAck
  : Specifies that a FastBack client operation that is identified by the ACTION parameter is to be scheduled for processing. The ACTION parameter must be either ARCHIVE or BACKUP.

  SYSTEMSTate
  : Specifies that a client Systemstate backup is scheduled.

  VApp
  : Specifies that a client vApp backup is scheduled. A vApp is a collection of pre-deployed virtual machines.

  VM
  : Specifies that a client VMware backup operation is scheduled.

Deploy
: Specifies whether to update client workstations with deployment packages that are specified with the OBJECTS parameter. The OBJECTS parameter must contain two specifications, the package files to retrieve and the location from which to retrieve them. Ensure that the objects are in the order *`files location`*. For example:

  ```
  define schedule standard deploy_1 action=DEPLOY objects=
  "\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\*
  ..\IBM_ANR_WIN\"
  ```

  Values for the following options are restricted when you specify ACTION=DEPLOY:

  PERUNITS
  : Specify `PERUNITS=ONETIME`. If you specify `PERUNITS=PERIOD`, the parameter is ignored.

  DURUNITS
  : Specify `MINUTES`, `HOURS`, or `DAYS` for the DURUNITS parameter. Do not specify INDEFINITE.

  SCHEDSTYLE
  : Specify the default style, CLASSIC.

The SCHEDULE command fails if the parameters do not conform to the required parameter values, such as the V.R.M.F.

OPTions

Specifies the client options that you specify to the scheduled command at the time the schedule is processed. This parameter is optional.

Only those options that are valid on the scheduled command can be specified for this parameter. Refer to the appropriate client manual for information about options that are valid from the command line. All options described there as valid only on the initial command line result in an error or are ignored when running the schedule from the server. For example, do not include the following options because they have no effect when the client processes the scheduled command:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

Windows When you define a scheduler service by using the DSMCUTIL command or the backup-archive client GUI wizard, you specify an options file. You cannot override the options in that options file by issuing the scheduled command. You must modify the options in your scheduler service.

If the option string contains multiple options or options with embedded spaces, surround the entire option string with one pair of apostrophes. Enclose individual options that contain spaces in quotation marks. A leading minus sign is required in front of the option. Errors can occur if the option string contains spaces that are not quoted correctly.

The following examples show how to specify some client options:

- To specify `subdir=yes` and `domain all-local -systemobject`, enter:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- To specify `domain all-local -c: -d:`, enter:
  - `options='-domain="all-local -c: -d:"'`

Windows Tip:

For Windows clients running in batch mode, if the use of quotation marks is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

- Processing a series of commands from the administrative client
- Processing individual commands from the administrative client

OBJects

Specifies the objects for which the specified action is performed. Use a single space between each object. This parameter is required except when ACTION=INCREMENTAL. If the action is a backup, archive, retrieve, or restore operation, the objects are file spaces, directories, or logical volumes. If the action is to run a command or macro, the object is the name of the command or macro to run.

When you specify ACTION=INCREMENTAL without specifying a value for this parameter, the scheduled command is invoked without specified objects and attempts to process the objects as defined in the client option file. To select all file spaces or directories for an action, explicitly list them in the object string. Entering only an asterisk in the object string causes the backup to occur only for the directory where the scheduler was started.

Important:

- If you specify a second file specification, and it is not a valid destination, you receive this error:

  ```
  ANS1082E Invalid destination file specification <filespec> entered.
  ```

- If you specify more than two file specifications, you receive this error:

  ```
  ANS1102E Excessive number of command line arguments passed to the
  program!
  ```

When you specify ACTION=ARCHIVE, INCREMENTAL, or SELECTIVE for this parameter, you can list a maximum of twenty (20) file specifications.

Enclose the object string in double quotes if it contains blank characters (spaces), and then surround the double quotes with single quotes. If the object string contains multiple file names, enclose each file name with its own pair of double quotes, then surround the entire string with one pair of single quotes. Errors can occur if file names contain a space that is not quoted correctly.

Windows If you are using characters that have a special meaning for Windows users, such as commas, surround the entire argument in two pairs of double quotes, then surround the entire string with single quotes. The following examples show you how to specify some file names:

- To specify C:\FILE 2, D:\GIF FILES, and E:\MY TEST FILE, enter:
  - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
- To specify D:\TEST FILE, enter:
  - `OBJECTS='"D:\TEST FILE"'`
- To specify D:TEST,FILE:
  - `OBJECTS='""D:\TEST,FILE""'`

AIX Linux The following examples show how to specify some file names:

- To specify /home/file 2, /home/gif files, and /home/my test file, enter:
  - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
- To specify /home/test file, enter:
  - `OBJECTS='"/home/test file"'`

Windows Tip:

For Windows clients running in batch mode, if the use of double quotes is necessary, use interactive mode or operating system escape characters. For additional information, see the following topics:

- Processing a series of commands from the administrative client
- Processing individual commands from the administrative client

PRIority
Specifies the priority value for a schedule. This parameter is optional. You can specify an integer from 1 to 10, with 1 being the highest priority and 10 being the lowest. The default is 5.

If two or more schedules have the same window start time, the value you specify determines when IBM Spectrum Protect™ processes the schedule. The schedule with the highest priority starts first. For example, a schedule with PRIORITY=3 starts before a schedule with PRIORITY=5.

STARTDate
Specifies the date for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current date. Use this parameter with the STARTTIME parameter to specify when the initial startup window of the schedule starts.
You can specify the date using one of the values below:

Value	Description	Example
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM

Value	Description	Example
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

STARTTime

Specifies the time for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current time. This parameter is used in conjunction with the STARTDATE parameter to specify when the initial startup window begins.

You can specify the time using one of the values below:

Value	Description	Example
HH:MM:SS	A specific time	10:30:08
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with STARTTIME=NOW+02:00 or STARTTIME=+02:00, the beginning of the startup window is at 7:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW-02:00 **or** -02:00. If you issue this command at 5:00 with STARTTIME=NOW-02:00 or STARTTIME=-02:00, the beginning of the startup window is at 3:00.

DURation

Specifies the number of units that define the length of the startup window of the scheduled operation. This parameter is optional. This value must be from 1 to 999. The default is 1.

Use this parameter with the DURUNITS parameter to specify the length of the startup window. For example, if you specify DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The default length of the startup window is 1 hour. The duration of the window must be shorter than the period between windows.

This value is ignored if you specify DURUNITS=INDEFINITE.

Tip: Define schedules with durations longer than 10 minutes. Doing this will give the IBM Spectrum Protect scheduler enough time to process the schedule and prompt the client.

DURUnits

Specifies the time units used to determine the duration of the window in which the schedule can start. This parameter is optional. The default is HOURS.

Use this parameter with the DURATION parameter to specify how long the startup window remains open to process the schedule. For example, if DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The schedule may not necessarily complete processing within this window. If the schedule needs to be retried for any reason, the retry attempts must begin before the startup window elapses, or the operation does not restart.

The default value for the length of the startup window is 1 hour. You can specify one of the following values:

Minutes
: Specifies that the duration of the window is defined in minutes.

Hours
: Specifies that the duration of the window is defined in hours.

Days
: Specifies that the duration of the window is defined in days.

INDefinite
: Specifies that the startup window of the scheduled operation has an indefinite duration. The schedule can run any time after the scheduled start time, until the schedule expires. You cannot specify DURUNITS=INDEFINITE, unless you specify PERUNITS=ONETIME. The INDEFINITE value is not allowed with enhanced schedules.

MAXRUNtime

Specifies the maximum run time, which is the number of minutes during which all client sessions that are started by the scheduled operation should be completed. If sessions are still running after the maximum run time, the server issues a warning message, but the sessions continue to run.
Tip: The maximum run time is calculated from the beginning of the startup window and not from the time that sessions start within the startup window.
Restrictions:

- The value of the parameter is not distributed to servers that are managed by an enterprise configuration manager.
- The value of the parameter is not exported by the EXPORT command.

The parameter is optional. You can specify a number in the range 0-1440. A value of 0 means that the maximum run time is indefinite, and no warning message is issued. The maximum run time must be greater than the startup window duration, which is defined by the DURATION and DURUNITS parameters.

For example, if the start time of a scheduled operation is 9:00 PM, and the duration of the startup window is 2 hours, the startup window is 9:00 PM - 11:00 PM. If the maximum run time is 240 minutes, that is, 4 hours, all client sessions for this operation should be completed by 1:00 AM. If one or more sessions are still running after 1:00 AM, the server issues a warning message.
Tip: Alternatively, you can specify a *run time alert* value of 1:00 AM in the IBM Spectrum Protect Operations Center.

SCHEDStyle

This parameter is optional. SCHEDSTYLE defines either the interval between times when a schedule can run, or the days on which it can run. The style can be either classic or enhanced. This parameter must be specified when you change a schedule from classic to enhanced or back to classic. Otherwise, the value for the existing schedule is used.

For classic schedules, these parameters are allowed: PERIOD, PERUNITS, and DAYOFWEEK. These parameters are not allowed: MONTH, DAYOFMONTH, and WEEKOFMONTH. If the previous schedule style was enhanced, the MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK parameters are reset. DAYOFWEEK, PERIOD, and PERUNITS are set to default values unless they are specified with the update command.

For enhanced schedules, these parameters are allowed: MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK. These parameters are not allowed: PERIOD and PERUNITS. If the previous schedule style was classic, the DAYOFWEEK, PERIOD, and PERUNITS parameters are reset. MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK are set to default values unless they are specified with the update command.

PERiod

Specifies the length of time between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. You can specify an integer from 1 to 999. The default is 1.

Use this parameter with the PERUNITS parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every five days after the initial start date and start time. The period between startup windows must exceed the duration of each window. The default is 1 day.

This value is ignored if you specify PERUNITS=ONETIME.

PERUnits

Specifies the time units used to determine the period between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. The default is DAYS.
Use this parameter with the PERIOD parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every 5 days after the initial start date and start time. The default is 1 day. You can specify one of the following values:

Hours
: Specifies that the time between startup windows is in hours.

Days
: Specifies that the time between startup windows is in days.

Weeks
: Specifies that the time between startup windows is in weeks.

Months
: Specifies that the time between startup windows is in months.

When you specify PERUNITS=MONTHS, the scheduled operation will be processed each month on the same date. For example, if the start date for the scheduled operation is 02/04/1998, the schedule will process on the 4th of every month thereafter. However, if the date is not valid for the next month, then the scheduled operation will be

processed on the last valid date in the month. Thereafter, subsequent operations are based on this new date. For example, if the start date is 03/31/1998, the next month's operation will be scheduled for 04/30/1998. Thereafter, all subsequent operations will be on the 30th of the month until February. Because February has only 28 days, the operation will be scheduled for 02/28/1999. Subsequent operations will be processed on the 28th of the month.

Years
: Specifies that the time between startup windows for the schedule is in years.

  When you specify PERUNITS=YEARS, the scheduled operation will be processed on the same month and date of each year. For example, if the start date for the scheduled operation is 02/29/2004, the next year's scheduled operation will be 02/28/2005 because February only has 28 days. Thereafter, subsequent operations will be scheduled for February 28th.

Onetime
: Specifies that the schedule processes once. This value overrides the value you specified for the PERIOD parameter.

DAYofweek
: Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can specify different options for the DAYofweek parameter, depending on whether the schedule style was defined as Classic or Enhanced:

  Classic Schedule
  : Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can either specify one day of the week, or WEEKDAY, WEEKEND, or ANY. If the start date and start time fall on a day that does not correspond to a day you specify, the start date and start time will be shifted forward in 24-hour increments until the DAYOFWEEK parameter is satisfied.

    If you select a value for DAYOFWEEK other than ANY, and depending on the values for PERIOD and PERUNITS, schedules may not be processed when you would expect. The default is ANY.

  Enhanced Schedule
  : Specifies the days of the week on which to run the schedule. You can either specify multiple days separated by commas and no intervening blanks, or WEEKDAY, WEEKEND, or ANY. If you specify multiple days, the schedule will run on each of the specified days. If you specify WEEKDAY or WEEKEND, you must also specify either WEEKOFMONTH=FIRST or WEEKOFMONTH=LAST, and the schedule will run just once per month.

    The default value is ANY, meaning the schedule will run every day of the week or on the day or days determined by other enhanced schedule parameters. DAYOFWEEK must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

  Possible values for the DAYofweek parameter are:

  ANY
  : Specifies that the startup window can begin on any day of the week.

  WEEKDay
  : Specifies that the startup window can begin on Monday, Tuesday, Wednesday, Thursday, or Friday.

  WEEKEnd
  : Specifies that the startup window can begin on Saturday or Sunday.

  SUnday
  : Specifies that the startup window begins on Sunday.

  Monday
  : Specifies that the startup window begins on Monday.

  TUesday
  : Specifies that the startup window begins on Tuesday.

  Wednesday
  : Specifies that the startup window begins on Wednesday.

  THursday
  : Specifies that the startup window begins on Thursday.

  Friday
  : Specifies that the startup window begins on Friday.

  SAturday
  : Specifies that the startup window begins on Saturday.

MONth

Specifies the months of the year during which to run the schedule. This parameter is used only with enhanced schedules. Specify multiple values by using commas and no intervening blanks. The default value is ANY, which means that the schedule runs during every month of the year.

DAYOFMonth

Specifies the day of the month to run the schedule. This parameter is used only with enhanced schedules. You can either specify ANY or a number from -31 through 31, excluding zero. Negative values are a day from the end of the month, counting backwards. For example, the last day of the month is -1, the next-to-the-last day of the month is -2. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule runs on each of the specified days of the month. If multiple values resolve to the same day, the schedule runs only once that day.

The default value is ANY, which means that the schedule runs on every day of the month or on the days determined by other enhanced schedule parameters. DAYOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFWEEK or WEEKOFMONTH parameters.

If an existing schedule specifies a value other than ANY for DAYOFWEEK and WEEKOFMONTH, and DAYOFMONTH is updated, DAYOFWEEK and WEEKOFMONTH are reset to ANY.

WEEKofmonth

Specifies the week of the month in which to run the schedule. This parameter is used only with enhanced schedules. A week is considered any seven-day period which does not start on a particular day of the week. You can specify FIRST, SECOND, THIRD, FOURTH, LAST, or ANY. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule runs during each of the specified weeks of the month. If multiple values resolve to the same week, the schedule runs only once during that week.

The default value is ANY. ANY means that the schedule runs during every week of the month or on the day or days determined by other enhanced schedule parameters. WEEKOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

EXPiration

Specifies the date after which this schedule is no longer used. This parameter is optional. The default is NEVER. You can specify one of the following values:

Never

Specifies that the schedule never expires.

expiration_date

Specifies the date on which this schedule expires, in MM/DD/YYYY format. If you specify an expiration date, the schedule expires at 23:59:59 on the date you specify.

Example: Update the priority of a schedule

Update the MONTHLY_BACKUP schedule that belongs to the STANDARD policy domain by setting its priority value to 1.

```
update schedule standard monthly_backup priority=1
```

Example: Update the expiration date of a schedule

Update the WEEKLY_BACKUP schedule that belongs to the EMPLOYEE_RECORDS policy domain to expire on March 29, 1999 (03/29/1999).

```
update schedule employee_records weekly_backup expiration=03/29/1999
```

Example: Update a schedule to archive on the last Friday of a month

Update a schedule from archiving files quarterly on the last Friday of the month to archiving on the last day of the specified months.

```
update schedule employee_records quarterly_archive dayofmonth=-1
```

WEEKOFMONTH and DAYOFWEEK are reset to ANY.

UPDATE SCHEDULE (Update an administrative schedule)

Use this command to update selected parameters for an administrative command schedule.

You cannot schedule MACRO or QUERY ACTLOG commands.

A managed administrative schedule that is updated by a configuration manager is set to an inactive state on the managed servers during configuration refresh processing. It remains in an inactive state until it is updated to an active state on those servers.

Privilege class

To update an administrative schedule, you must have system privilege.

Syntax

```
Classic administrative schedule

                     (1)
>>-UPDate SCHedule--------schedule_name-------------------------->

>--+-------------------------+--+-----------------+------------->
   '-Type--=--Administrative-'  '-CMD--=--command-'

>--+--------------------+--+-----------------------------+------>
   '-ACTIVE--=--+-Yes-+-'  '-DESCription--=--description-'
                '-No--'

>--+---------------------+--+--------------------+-------------->
   '-PRIority--=--number-'  '-STARTDate--=--date-'

>--+--------------------+--+---------------------+-------------->
   '-STARTTime--=--time-'  '-DURation--=--number-'

>--+-----------------------------+--+-----------------------+--->
   '-DURUnits--=--+-Minutes----+-'  '-MAXRUNtime--=--number-'
                  +-Hours------+
                  +-Days-------+
                  '-INDefinite-'

>--+------------------------+--+-------------------+------------>
   '-SCHEDStyle--=--Classic-'  '-PERiod--=--number-'

>--+--------------------------+-------------------------------->
   '-PERUnits--=--+-Hours---+-'
                  +-Days----+
                  +-Weeks---+
                  +-Months--+
                  +-Years---+
                  '-Onetime-'

>--+-----------------------------+------------------------------>
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+------------------------+--------------------------------><
   '-EXPiration=--+-Never-+-'
                  '-date--'
```

Notes:

1. You must specify at least one optional parameter on this command.

Syntax

Enhanced administrative schedule

Notes:

1. You must specify at least one optional parameter on this command.

Parameters

schedule_name (Required)
Specifies the name of the schedule to be updated.
Type=Administrative (Required)

Specifies that an administrative command schedule is updated.

CMD

Specifies the administrative command to be scheduled for processing. This parameter is optional. The command you specify can contain up to 512 characters. Enclose the command in quotation marks if it contains blanks.

You cannot specify redirection characters with this parameter.

ACTIVE

Specifies whether the administrative command is eligible for processing. This parameter is optional. An administrative command schedule will not be processed unless it is set to the active state. Possible values are:

YES

Specifies that the administrative command is eligible for processing.

NO

Specifies that the administrative command is not eligible for processing.

DESCription

Specifies a description of the schedule. This parameter is optional. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains blanks. To remove a previously defined description, specify a null string ("") for this value.

PRIority

Specifies the priority value for a schedule. This parameter is optional. You can specify an integer from 1 to 10, with 1 being the highest priority and 10 being the lowest. The default is 5.

If two or more schedules have the same window start time, the value you specify determines when IBM Spectrum Protect™ processes the schedule. The schedule with the highest priority starts first. For example, a schedule with PRIORITY=3 starts before a schedule with PRIORITY=5.

STARTDate

Specifies the date for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current date. Use this parameter with the STARTTIME parameter to specify when the initial startup window of the schedule starts.

You can specify the date using one of the values below:

Value	**Description**	**Example**
MM/DD/YYYY	A specific date	09/15/1998
TODAY	The current date	TODAY
TODAY+days **or** +days	The current date plus days specified. The maximum number of days you can specify is 9999.	TODAY +3 **or** +3.
EOLM (End Of Last Month)	The last day of the previous month.	EOLM
EOLM-days	The last day of the previous month minus days specified.	EOLM-1 To include files that were active a day before the last day of the previous month.
BOTM (Beginning Of This Month)	The first day of the current month.	BOTM
BOTM+days	The first day of the current month, plus days specified.	BOTM+9 To include files that were active on the 10th day of the current month.

STARTTime

Specifies the time for the beginning of the window in which the schedule is first processed. This parameter is optional. The default is the current time. This parameter is used in conjunction with the STARTDATE parameter to specify when the initial startup window begins.

You can specify the time using one of the values below:

Value	**Description**	**Example**
HH:MM:SS	A specific time	10:30:08

Value	Description	Example
NOW	The current time	NOW
NOW+HH:MM **or** +HH:MM	The current time plus hours and minutes specified	NOW+02:00 **or** +02:00. If you issue this command at 5:00 with STARTTIME=NOW+02:00 or STARTTIME=+02:00, the beginning of the startup window is at 7:00.
NOW-HH:MM **or** -HH:MM	The current time minus hours and minutes specified	NOW-02:00 **or** -02:00. If you issue this command at 5:00 with STARTTIME=NOW-02:00 or STARTTIME=-02:00, the beginning of the startup window is at 3:00.

DURation
: Specifies the number of units that define the length of the startup window of the scheduled operation. This parameter is optional. This value must be from 1 to 999. The default is 1.

  Use this parameter with the DURUNITS parameter to specify the length of the startup window. For example, if you specify DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The default length of the startup window is 1 hour. The duration of the window must be shorter than the period between windows.

  This value is ignored if you specify DURUNITS=INDEFINITE.

DURUnits
: Specifies the time units used to determine the duration of the window in which the schedule can start. This parameter is optional. The default is HOURS.

  Use this parameter with the DURATION parameter to specify how long the startup window remains open to process the schedule. For example, if DURATION=20 and DURUNITS=MINUTES, the schedule must be started within 20 minutes of the start date and start time. The schedule may not necessarily complete processing within this window. If the schedule needs to be retried for any reason, the retry attempts must begin before the startup window elapses, or the operation does not restart.

  The default value for the length of the startup window is 1 hour. You can specify one of the following values:

  Minutes
  : Specifies that the duration of the window is defined in minutes.

  Hours
  : Specifies that the duration of the window is defined in hours.

  Days
  : Specifies that the duration of the window is defined in days.

  INDefinite
  : Specifies that the startup window of the scheduled operation has an indefinite duration. The schedule can run any time after the scheduled start time, until the schedule expires. You cannot specify DURUNITS=INDEFINITE, unless you specify PERUNITS=ONETIME. The INDEFINITE value is not allowed with enhanced schedules.

MAXRUNtime
: Specifies the maximum run time, which is the number of minutes during which server processes that are started by the scheduled commands must be completed. If processes are still running after the maximum run time, the central scheduler cancels the processes.
  Tips:

  - The processes might not end immediately when the central scheduler cancels them; they end when they register the cancellation notification from the central scheduler.
  - The maximum run time is calculated beginning from when the server process starts. If the schedule command starts more than one process, each process maximum run time is calculated from when the process starts.
  - This parameter does not apply to some processes, such as duplicate-identification processes, which can continue to run after the maximum run time.
  - This parameter does not apply if the scheduled command does not start a server process.
  - Another cancel time might be associated with some commands. For example, the MIGRATE STGPOOL command can include a parameter that specifies the length of time that the storage pool migration runs before the migration is

automatically canceled. If you schedule a command for which a cancel time is defined, and you also define a maximum run time for the schedule, the processes are canceled at whichever cancel time is reached first.

Restrictions:

- The value of the parameter is not distributed to servers that are managed by an enterprise configuration manager.
- The value of the parameter is not exported by the EXPORT command.

This parameter is optional. You can specify a number in the range 0-1440. A value of 0 means that the maximum run time is indefinite, and the central scheduler does not cancel processes. The maximum run time must be greater than the startup window duration, which is defined by the DURATION and DURUNITS parameters.

For example, if the start time of a scheduled command is 9:00 PM, and the duration of the startup window is 2 hours, the startup window is 9:00 PM - 11:00 PM. If the maximum run time is 240 minutes, that is, 4 hours, all applicable server processes that are started by the command must be completed by 1:00 AM. If one or more applicable processes are still running after 1:00 AM, the central scheduler cancels the processes.
Tip: Alternatively, you can specify an *end time* of 1:00 AM in the IBM Spectrum Protect Operations Center.

SCHEDStyle
: This parameter is optional. SCHEDSTYLE defines either the interval between times when a schedule should run, or the days on which it should run. The style can be either classic or enhanced. This parameter must be specified when you change a schedule from classic to enhanced or back to classic. Otherwise, the value for the existing schedule is used.

  For classic schedules, these parameters are allowed: PERIOD, PERUNITS, and DAYOFWEEK. These parameters are not allowed: MONTH, DAYOFMONTH, and WEEKOFMONTH. If the previous schedule style was enhanced, the MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK parameters will be reset. DAYOFWEEK, PERIOD, and PERUNITS will be set to default values unless they are specified with the update command.

  For enhanced schedules, these parameters are allowed: MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK. These parameters are not allowed: PERIOD and PERUNITS. If the previous schedule style was classic, the DAYOFWEEK, PERIOD, and PERUNITS parameters will be reset. MONTH, DAYOFMONTH, WEEKOFMONTH, and DAYOFWEEK will be set to default values unless they are specified with the update command.

PERiod
: Specifies the length of time between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. You can specify an integer from 1 to 999. The default is 1.

  Use this parameter with the PERUNITS parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every five days after the initial start date and start time. The period between startup windows must exceed the duration of each window. The default is 1 day.

  This value is ignored if you specify PERUNITS=ONETIME.

PERUnits
: Specifies the time units used to determine the period between startup windows for this schedule. This parameter is optional. This parameter is used only with classic schedules. The default is DAYS.
  Use this parameter with the PERIOD parameter to specify the period between startup windows. For example, if you specify PERIOD=5 and PERUNITS=DAYS (assuming that DAYOFWEEK=ANY), the operation is scheduled every 5 days after the initial start date and start time. The default is 1 day. You can specify one of the following values:

  Hours
  : Specifies that the time between startup windows is in hours.

  Days
  : Specifies that the time between startup windows is in days.

  Weeks
  : Specifies that the time between startup windows is in weeks.

  Months
  : Specifies that the time between startup windows is in months.

    When you specify PERUNITS=MONTHS, the scheduled operation will be processed each month on the same date. For example, if the start date for the scheduled operation is 02/04/1998, the schedule will process on the 4th of every month thereafter. However, if the date is not valid for the next month, then the scheduled operation will be processed on the last valid date in the month. Thereafter, subsequent operations are based on this new date. For example, if the start date is 03/31/1998, the next month's operation will be scheduled for 04/30/1998. Thereafter,

all subsequent operations will be on the 30th of the month until February. Because February has only 28 days, the operation will be scheduled for 02/28/1999. Subsequent operations will be processed on the 28th of the month.

Years
: Specifies that the time between startup windows for the schedule is in years.

  When you specify PERUNITS=YEARS, the scheduled operation will be processed on the same month and date of each year. For example, if the start date for the scheduled operation is 02/29/2004, the next year's scheduled operation will be 02/28/2005 because February only has 28 days. Thereafter, subsequent operations will be scheduled for February 28th.

Onetime
: Specifies that the schedule processes once. This value overrides the value you specified for the PERIOD parameter.

DAYofweek
: Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can specify different options for the DAYofweek parameter, depending on whether the schedule style was defined as Classic or Enhanced:

  Classic Schedule
  : Specifies the day of the week on which the startup window for the schedule begins. This parameter is optional. You can either specify one day of the week, or WEEKDAY, WEEKEND, or ANY. If the start date and start time fall on a day that does not correspond to a day you specify, the start date and start time will be shifted forward in 24-hour increments until the DAYOFWEEK parameter is satisfied.

    If you select a value for DAYOFWEEK other than ANY, and depending on the values for PERIOD and PERUNITS, schedules may not be processed when you would expect. The default is ANY.

  Enhanced Schedule
  : Specifies the days of the week on which to run the schedule. You can either specify multiple days separated by commas and no intervening blanks, or WEEKDAY, WEEKEND, or ANY. If you specify multiple days, the schedule will run on each of the specified days. If you specify WEEKDAY or WEEKEND, you must also specify either WEEKOFMONTH=FIRST or WEEKOFMONTH=LAST, and the schedule will run just once per month.

    The default value is ANY, meaning the schedule will run every day of the week or on the day or days determined by other enhanced schedule parameters. DAYOFWEEK must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

  Possible values for the DAYofweek parameter are:

  ANY
  : Specifies that the startup window can begin on any day of the week.

  WEEKDay
  : Specifies that the startup window can begin on Monday, Tuesday, Wednesday, Thursday, or Friday.

  WEEKEnd
  : Specifies that the startup window can begin on Saturday or Sunday.

  SUnday
  : Specifies that the startup window begins on Sunday.

  Monday
  : Specifies that the startup window begins on Monday.

  TUesday
  : Specifies that the startup window begins on Tuesday.

  Wednesday
  : Specifies that the startup window begins on Wednesday.

  THursday
  : Specifies that the startup window begins on Thursday.

  Friday
  : Specifies that the startup window begins on Friday.

  SAturday
  : Specifies that the startup window begins on Saturday.

MONth
: Specifies the months of the year during which to run the schedule. This parameter is used only with enhanced schedules. Specify multiple values by using commas and no intervening blanks. The default value is ANY. This means the schedule will run during every month of the year.

DAYOFMonth
: Specifies the day of the month to run the schedule. This parameter can only be specified with enhanced schedules. You can either specify ANY or a number from -31 through 31, excluding zero. Negative values are a day from the end of the month, counting backwards. For example, the last day of the month is -1, the next-to-the-last day of the month is -2, etc. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule will run on each of the specified days of the month. If multiple values resolve to the same day, the schedule will run only once that day.

  The default value is ANY. This means the schedule will run on every day of the month or on the days determined by other enhanced schedule parameters. DAYOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFWEEK or WEEKOFMONTH parameters.

WEEKofmonth
: Specifies the week of the month in which to run the schedule. This parameter can only be specified with enhanced schedules. A week is considered any seven-day period which does not start on a particular day of the week. You can specify FIRST, SECOND, THIRD, FOURTH, LAST, or ANY. You can specify multiple values separated by commas and no intervening blanks. If you specify multiple values, the schedule will run during each of the specified weeks of the month. If multiple values resolve to the same week, the schedule will run only once during that week.

  The default value is ANY, meaning the schedule will run during every week of the month or on the day or days determined by other enhanced schedule parameters. WEEKOFMONTH must have a value of ANY (either by default or specified with the command) when used with the DAYOFMONTH parameter.

EXPiration
: Specifies the date after which this schedule is no longer used. This parameter is optional. The default is NEVER. You can specify one of the following values:

  Never
  : Specifies that the schedule never expires.

  expiration_date
  : Specifies the date on which this schedule expires, in MM/DD/YYYY format. If you specify an expiration date, the schedule expires at 23:59:59 on the date you specify.

Example: Update a backup schedule to every three days

Update existing administrative schedule named BACKUP_BACKUPPOOL so that starting today, the BACKUPPOOL primary storage pool is backed up to the COPYSTG copy storage pool every three days at 10:00 p.m.

```
update schedule backup_backuppool type=administrative cmd="backup stgpool
    backuppool copystg" active=yes starttime=22:00 period=3
```

Example: Update a backup schedule to every first and third Friday

Update a schedule named BACKUP_ARCHIVEPOOL that backs up the primary storage pool ARCHIVEPOOL to the copy storage pool RECOVERYPOOL. The existing schedule runs on the first and tenth day of every month. Update it to run the first and third Friday of every month.

```
update schedule backup_archivepool
dayofweek=friday weekofmonth=first,third
```

DAYOFMONTH will be reset to ANY.

UPDATE SCRATCHPADENTRY (Update a scratch pad entry)

Use this command to update data on a line in the scratch pad.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UPDate SCRATCHPadentry--major_category--minor_category------->
```

```
>--subject--Line--=--number--Data--=--data--------------------><
```

Parameters

major_category (Required)
: Specifies the major category in which data is to be updated. This parameter is case sensitive.

minor_category (Required)
: Specifies the minor category in which data is to be updated. This parameter is case sensitive.

subject (Required)
: Specifies the subject under which data is to be updated. This parameter is case sensitive.

Line (Required)
: Specifies the number of the line on which data is to be updated.

Data (Required)
: Specifies the new data to be stored on the line. Previous data is deleted. You can enter up to 1000 characters. Enclose the data in quotation marks if the data contains one or more blanks. The data is case sensitive.

Example: Update a scratch pad entry

Update the vacation contact details of an administrator, Jane, in a database that stores information about the location of all administrators:

```
update scratchpadentry admin_info location jane line=2 data=
"Out of the office until 18 Nov."
```

Related commands

Table 1. Commands related to UPDATE SCRATCHPADENTRY

Command	Description
DEFINE SCRATCHPADENTRY	Creates a line of data in the scratch pad.
DELETE SCRATCHPADENTRY	Deletes a line of data from the scratch pad.
QUERY SCRATCHPADENTRY	Displays information that is contained in the scratch pad.
SET SCRATCHPADRETENTION	Specifies the amount of time for which scratch pad entries are retained.

UPDATE SCRIPT (Update an IBM Spectrum Protect script)

Use this command to change a command line or to add a new command line to an IBM Spectrum Protect™ script.

Restriction: You cannot redirect the output of a command within an IBM Spectrum Protect script. Instead, run the script and then specify command redirection. For example, to direct the output of script1 to the c:\temp\test.out directory, run the script and specify command redirection as in the following example:

```
run script1 > c:\temp\test.out
```

Privilege class

To issue this command, the administrator must have previously defined the script or must have system privilege.

Syntax

```
>>-UPDate SCRipt--script_name----------------------------------->

>--+-----------------------------------+------------------------>
   '-command_line--+-----------------+-'
                   '-Line--=--number-'

>--+---------------------------+---------------------------><
```

```
'-DESCription--=--description-'
```

Parameters

script_name (Required)
: Specifies the name of the script to be updated.

command_line
: Specifies a new or updated command to be processed in a script. You must update a command, a description, or both when you issue this command.

  Command can contain substitution variables and may be continued across multiple lines if you specify a continuation character (-) as the last character in the command. You can specify up to 1200 characters for the command. Enclose the command in quotation marks if it contains blanks. If you specify this parameter, you can optionally specify the following parameter.

  You have the options of running commands serially, in parallel, or serially and in parallel by specifying the SERIAL or PARALLEL script commands for this parameter. You can run multiple commands in parallel and wait for them to complete before proceeding to the next command. Commands will run serially until the parallel command is encountered.

  Conditional logic flow statements can be used. These statements include IF, EXIT, and GOTO.

  Line
  : Specifies the line number for the command. If you do not specify a line number, the command line is appended to the existing series of command lines. The appended command line is assigned a line number of five greater than the last command line number in the sequence. For example, if the last line in your script is 015, the appended command line is assigned a line number of 020.

    If you specify a line number, the command will replace an existing line (if the number is the same as an existing line). Or the command will insert the specified line (if the line number does not correspond to an existing line number for the command line sequence).

DESCription
: Specifies a description for the script. You can specify up to 255 characters for the description. Enclose the description in quotation marks if it contains blank characters.

Example: Add a command to the end of a script

Assume that you have defined the following three line script, named QSAMPLE, and that you want to add the QUERY SESSION command to the end of the script.

```
001  /* This is a sample script */
005  QUERY STATUS
010  QUERY PROCESS
```

```
update script qsample "query session"
```

After the command processes, the script now consists of the following lines:

```
001  /* This is a sample script */
005  QUERY STATUS
010  QUERY PROCESS
015  QUERY SESSION
```

Example: Update a specific line a script

Using the script from the prior example, change line 010 so that it processes the QUERY STGPOOL command instead of the QUERY PROCESS command:

```
update script qsample "query stgpool" line=010
```

After the command processes, the script now consists of the following lines:

```
001  /* This is a sample script */
005  QUERY STATUS
```

```
010  QUERY STGPOOL
015  QUERY SESSION
```

Example: Insert a command in the middle of a script

Using the script from the prior example, insert a new command line (QUERY NODE) after the QUERY STATUS command line in the QSAMPLE script:

```
update script qsample "query node"
line=007
```

After the command processes, the script now consists of the following lines:

```
001  /* This is a sample script */
005  QUERY STATUS
007  QUERY NODE
010  QUERY STGPOOL
015  QUERY SESSION
```

Related commands

Table 1. Commands related to UPDATE SCRIPT

Command	Description
COPY SCRIPT	Creates a copy of a script.
DEFINE SCRIPT	Defines a script to the IBM Spectrum Protect server.
DELETE SCRIPT	Deletes the script or individual lines from the script.
QUERY SCRIPT	Displays information about scripts.
RENAME SCRIPT	Renames a script to a new name.
RUN	Runs a script.

Related tasks:
Running commands in parallel or serially
Including logic flow statements in a script
Performing tasks concurrently on multiple servers
Defining a server script
Related reference:
Return codes for use in IBM Spectrum Protect scripts

UPDATE SERVER (Update a server defined for server-to-server communications)

Use this command to update a server definition.

Restriction: If this server is a source server for a virtual volume operation, changing any of these values can affect the ability of the source server to access and manage the data that is stored on the corresponding target server. Changing the server name by using the SET SERVERNAME command might have additional implications, varying by operating system. The following are some examples:

- Passwords might be invalidated
- Device information might be affected
- Registry information about Windows operating systems might change

Privilege class

To issue this command, you must have system privilege.

Syntax for:

- **Enterprise configuration**

- **Enterprise event logging**
- **Command routing**
- **Storage agent**
- **Node replication source and target servers**
- AIX Linux **z/OS® media server**

```
>>-UPDate--SERver--server_name---------------------------------->

>--+-----------------------------+------------------------------>
   '-SERVERPAssword--=--password-'

>--+--------------------------+--+-----------------------+----->
   '-HLAddress--=--ip_address-'  '-LLAddress--=--tcp_port-'

>--+----------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--url-'

>--+---------------------------+------------------------------->
   '-ALLOWReplace--=--+-Yes-+-'
                      '-No--'

>--+-----------------------------+--+-----------------------+--->
   '-DESCription--=--description-'  '-FORCESync--=--+-Yes-+-'
                                                   '-No--'

>--+-----------------------------------+---------------------->
   |  (1)                              |
   '-------VALIdateprotocol--=--+-No--+-'
                                '-All-'

>--+-----------------+------------------------------------------>
   '-SSL--=--+-No--+-'
             '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+--------------------------------------+---------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------------+------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (2) |
                        '-Fasp-----'
```

Notes:

1. The VALIDATEPROTOCOL parameter is deprecated and applies only to storage agent definitions.
2. Linux The TRANSFERMETHOD parameter is available only on Linux x86_64 operating systems.

Syntax for virtual volumes

```
>>-UPDate--SERver--server_name--+----------------------+------->
                                '-PAssword--=--password-'

>--+--------------------------+--+-----------------------+----->
   '-HLAddress--=--ip_address-'  '-LLAddress--=--tcp_port-'

>--+----------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--url-'

>--+------------------------+--+-----------------------+------>
   '-DELgraceperiod--=--days-'  '-NODEName--=--node_name-'

                    .-SESSIONSECurity--=--TRANSitional-----.
>--+-------------+--+--------------------------------------+---->
   '-SSL--=--Yes-'  '-SESSIONSECurity--=--+-STRict-------+-'
                                          '-TRANSitional-'
```

```
>--+-----------------------+--+-----------------------------+--><
   '-FORCESync--=--+-Yes-+-'  '-DESCription--=--description-'
                   '-No--'
```

Parameters

server_name (Required)
: Specifies the name of the server to be updated. This parameter is required.

PAssword
: Specifies the password that is used to sign on to the target server for virtual volumes. This parameter is optional. If you specify a password, the minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

SERVERPAssword
: Specifies the server password, which is used for enterprise configuration, command routing, and server-to-server event logging functions. The password must match the server password that is set by the SET SERVERPASSWORD command. This parameter is optional. The minimum length of the password is 8 characters unless a different value is specified by using the SET MINPWLENGTH command. The maximum length of the password is 64 characters.

HLAddress
: Specifies the IP address (in dotted decimal format) of the server. This parameter is optional.

LLAddress
: Specifies the low-level address of the server. This address is usually the same as the address in the TCPPORT server option of the target server. When SSL=YES, the port must already be designated for SSL communications on the target server.

COMMmethod
: Specifies the communication method that is used to connect to the server. This parameter is optional.

URL
: Specifies the URL address that is used to access this server from the Administration Center. The parameter is optional.

DELgraceperiod
: Specifies a number of days that an object remains on the target server after it was marked for deletion. You can specify a value 0 - 9999. The default is 5. This parameter is optional.

NODEName
: Specifies a node name to be used by the server to connect to the target server. This parameter is optional.

DESCription
: Specifies a description of the server. This parameter is optional. The description can be up to 255 characters. Enclose the description in quotation marks if it contains blank characters. To remove an existing description, specify a null string ('').

FORCESync
: Specifies whether to reset the server verification key when the source server next signs on to the target server. A valid verification key enables a source server to put objects on the target server, manage the grace deletion period value, and update the password, if the current password is known and the verification key matches. The parameter is optional. You can specify one of the following values:

  Yes
  : Specifies that a new verification key will be sent to and accepted by the target server if a valid password is received.

  No
  : Specifies that a new verification key will not be sent to the target server.

VALIdateprotocol (deprecated)
: Specifies whether a cyclic redundancy check validates the data sent between the storage agent and the IBM Spectrum Protect™ server. The parameter is optional. The default is NO.
  Important: Beginning with IBM Spectrum Protect Version 8.1.2 and Tivoli® Storage Manager Version 7.1.8, validation that is enabled by this parameter is replaced by the TLS 1.2 protocol, which is enforced by the SESSIONSECURITY parameter. The VALIDATEPROTOCOL parameter is ignored. Update your configuration to use the SESSIONSECURITY parameter.

ALLOWReplace
: Specifies whether a server definition that was defined by a managed server can be replaced with a definition from the configuration manager. This parameter is optional. You can specify one of the following values:

  Yes
  : Specifies that a server definition can be replaced by a definition from the configuration manager.

  No
  : Specifies that a server definition cannot be replaced by the definition from the configuration manager.

SSL
: Specifies the communication mode of the server.

Important: Beginning with IBM Spectrum Protect V8.1.2 and Tivoli Storage Manager V7.1.8, SSL is used to encrypt some communication with the specified server even when you specify NO.
The following conditions and considerations apply when you specify the SSL parameter:

- Before starting the servers, self-signed certificates of the partner servers must be in the key database file (cert.kdb) of each of the servers.
- You can define multiple server names with different parameters for the same target server.

You can specify one of the following values:

No
: Specifies an SSL session for all communication with the specified server, except when the server is sending or receiving object data. Object data is sent and received by using TCP/IP. By choosing not to encrypt the object data, server performance is similar to communication over a TCP/IP session and the session is secure.

Yes
: Specifies an SSL session for all communication with the specified server, even when the server is sending and receiving object data.

SESSIONSECurity
: Specifies whether the server that you are defining must use the most secure settings to communicate with an IBM Spectrum Protect server. This parameter is optional.

You can specify one of the following values:

STRict
: Specifies that the strictest security settings are enforced for the server that you are defining. The STRICT value uses the most secure communication protocol available, which is currently TLS 1.2. The TLS 1.2 protocol is used for SSL sessions between the specified server and an IBM Spectrum Protect server.
To use the STRICT value, the following requirements must be met to ensure that the specified server can authenticate with the IBM Spectrum Protect server:

- Both the server that you are defining and the IBM Spectrum Protect server must be using IBM Spectrum Protect software that supports the SESSIONSECURITY parameter.
- The server that you are defining must be configured to use the TLS 1.2 protocol for SSL sessions between itself and the IBM Spectrum Protect server.

Servers set to STRICT that do not meet these requirements are unable to authenticate with the IBM Spectrum Protect server.

TRANSitional
: Specifies that the existing security settings are enforced for the server. This is the default value. This value is intended to be used temporarily while you update your security settings to meet the requirements for the STRICT value.

If SESSIONSECURITY=TRANSITIONAL and the server has never met the requirements for the STRICT value, the server will continue to authenticate by using the TRANSITIONAL value. However, after a server meets the requirements for the STRICT value, the SESSIONSECURITY parameter value automatically updates from TRANSITIONAL to STRICT. Then, the server can no longer authenticate by using a version of the client or an SSL/TLS protocol that does not meet the requirements for STRICT. In addition, after a server successfully authenticates by using a more secure communication protocol, the server can no longer authenticate by using a less secure protocol. For example, if a server that is not using SSL is updated and successfully authenticates by using TLS 1.2, the server can no longer authenticate by using no SSL protocol or TLS 1.1. This restriction also applies when you use functions such as virtual volumes, command routing, or server-to-server export, when a node or administrator authenticates to the IBM Spectrum Protect server as a node or administrator from another server.

Linux TRANSFERMethod
: Linux Specifies the method that is used for server-to-server data transfer. This parameter is optional. You can specify one of the following values:

Tcpip
: Specifies that TCP/IP is used to transfer data. This is the default.

Fasp
: Specifies that Aspera® Fast Adaptive Secure Protocol (FASP®) technology is used to transfer data. Aspera FASP technology can help you optimize data transfer in a wide area network (WAN).
Restrictions:

- Before you enable Aspera FASP technology, determine whether the technology is appropriate for your system environment and install the appropriate licenses. For instructions, see Determining whether Aspera FASP technology can optimize data transfer in your system environment. If the licenses are missing or expired, data transfer operations fail.
- If WAN performance meets your business needs, do not enable Aspera FASP technology.
- If you specify TRANSFERMETHOD=FASP on the PROTECT STGPOOL or REPLICATE NODE command, that value overrides the TRANSFERMETHOD parameter on the DEFINE SERVER and UPDATE SERVER commands.

Example: Update a deletion grace period for a server

Update the definition of SERVER2 to specify that objects remain on the target server for 10 days after they were marked for deletion.

```
update server server2 delgraceperiod=10
```

Example: Update the URL for a server

Update the definition of NEWSERVER to specify its URL address to be http://newserver:1580/.

```
update server newserver url=http://newserver:1580/
```

Example: Update all servers to communicate with an IBM Spectrum Protect server by using strict session security

Update the definition of all servers to use the strictest security settings to authenticate with the IBM Spectrum Protect server.

```
update server * sessionsecurity=strict
```

Related commands

Table 1. Commands related to UPDATE SERVER

Command	Description
DEFINE DEVCLASS	Defines a device class.
DEFINE SERVER	Defines a server for server-to-server communications.
DELETE DEVCLASS	Deletes a device class.
DELETE FILESPACE	Deletes data associated with client file spaces. If a file space is part of a collocation group and you remove the file space from a node, the file space is removed from the collocation group.
DELETE SERVER	Deletes the definition of a server.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY SERVER	Displays information about servers.
RECONCILE VOLUMES	Reconciles source server virtual volume definitions and target server archive objects.
REGISTER NODE	Defines a client node to the server and sets options for that user.
REMOVE NODE	Removes a client from the list of registered nodes for a specific policy domain.
UPDATE DEVCLASS	Changes the attributes of a device class.
UPDATE NODE	Changes the attributes that are associated with a client node.

UPDATE SERVERGROUP (Update a server group description)

Use this command to update the description of a server group.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-UPDate SERVERGroup--group_name------------------------------>

>--DESCription--=--description---------------------------------><
```

Parameters

group_name (Required)
: Specifies the server group to update.

DESCription (Required)
: Specifies a description of the server group. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains blank characters.

Example: Update the description of a server group

Update the description of the server group named WEST_COMPLEX to "Western Region Complex".

```
update servergroup west_complex
 description="western region complex"
```

Related commands

Table 1. Commands related to UPDATE SERVERGROUP

Command	Description
COPY SERVERGROUP	Creates a copy of a server group.
DEFINE SERVERGROUP	Defines a new server group.
DELETE SERVERGROUP	Deletes a server group.
QUERY SERVERGROUP	Displays information about server groups.
RENAME SERVERGROUP	Renames a server group.

UPDATE SPACETRIGGER (Update the space triggers)

Use this command to update settings for triggers that determine when and how the server resolves space shortages in storage pools that use sequential-access FILE and random-access DISK device classes.

For storage pools with a parameter RECLAMATIONTYPE=SNAPLOCK, space triggers are not enabled.

Important: Space trigger functions and storage pool space calculations take into account the space remaining in each directory. Ideally, you associate each directory with a separate file system. If you specify multiple directories for a device class and the directories reside in the same file system, the server calculates space by adding values representing the space remaining in each directory. These space calculations will be inaccurate. Rather than choosing a storage pool with sufficient space for an operation, the server might choose the wrong storage pool and run out of space prematurely. For space triggers, an inaccurate calculation might result in a failure to expand the space available in a storage pool. Failure to expand space in a storage pool is one of the conditions that can cause a trigger to become disabled. If a trigger is disabled because the space in a storage pool could not be expanded, you can re-enable the trigger by specifying the following command: `update spacetrigger stg`. No further changes are required to the space trigger.

See the DEFINE SPACETRIGGER command for more information.

Privilege class

To issue this command, you must have system privilege or unrestricted storage privilege.

Syntax

```
>>-UPDate SPACETrigger--STG--+--------------------+------------>
                            '-Fullpct--=--percent-'

>--+---------------------------+------------------------------>
   '-SPACEexpansion--=--percent-'

>--+---------------------------+------------------------------>
   '-EXPansionprefix--=--prefix-'

>--+-----------------------------+--------------------------><
   '-STGPOOL--=--storage_pool_name-'
```

Parameters

STG (Required)
: Specifies a storage pool space trigger

Fullpct
: This parameter specifies the utilization percentage of the storage pool.

  When this value is exceeded, the space trigger creates new volumes.

  You can determine storage pool utilization by issuing the QUERY STGPOOL command with FORMAT=DETAILED. The percentage of storage pool utilization for the storage pool is displayed in the field "Space Trigger Util." The calculation for this percentage does not include potential scratch volumes. The calculation for the percentage utilization used for migration and reclamation, however, does include potential scratch volumes.

SPACEexpansion
: For space triggers for sequential-access FILE-type storage pools, this parameter is used in determining the number of additional volumes that are created in the storage pool. Volumes are created using the MAXCAPACITY value from the storage pool's device class. For space triggers for random-access DISK storage pools, the space trigger creates a single volume using the EXPANSIONPREFIX.

EXPansionprefix
: This specifies the prefix that the server uses to create new storage pool files. This parameter is optional and applies only to random-access DISK device classes. The default prefix is the server installation path.
  The prefix can include one or more directory separator characters, for example: AIX Linux

  ```
  /opt/tivoli/tsm/server/bin/
  ```

  Windows

  ```
  c:\program files\tivoli\tsm\
  ```

  AIX Linux You can specify up to 250 characters. If you specify a prefix that is not valid, automatic expansion can fail.

  Windows You can specify up to 200 characters. If the server is running as a Windows service, the default prefix is the c:\wnnt\system32 directory. If you specify a prefix that is not valid, automatic expansion can fail.

  This parameter is not valid for space triggers for sequential-access FILE storage pools. Prefixes are obtained from the directories specified with the associated device class.

STGPOOL
: Specifies the storage pool associated with this space trigger. If the STGPOOL parameter is not specified, the default storage pool space trigger is updated.

  This parameter does not apply to storage pools with the parameter RECLAMATIONTYPE=SNAPLOCK.

Example: Increase the amount of space for a storage pool

Increase the amount of space in a storage pool by 50 percent when it is filled to 80 percent utilization of existing volumes. Space will be created in the directories associated with the device class.

```
update spacetrigger stg spaceexpansion=50 stgpool=file
```

Related commands

Table 1. Commands related to UPDATE SPACETRIGGER

Command	Description
DEFINE SPACETRIGGER	Defines a space trigger to expand the space for a storage pool.
DELETE SPACETRIGGER	Deletes the storage pool space trigger.
QUERY SPACETRIGGER	Displays information about a storage pool space trigger.

UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)

Use this command to update an existing status monitoring threshold.

Status monitoring thresholds compare the defined conditions to the status monitoring server queries and inserts the results in the status monitoring table.

Multiple thresholds can be defined for an activity. For example, you can create a threshold that provides a warning status if storage pool capacity utilization is greater than 80%. You can then create another threshold that provides error status if storage pool capacity utilization is greater than 90%.

Note: If a threshold is already defined for an EXISTS condition, you cannot define another threshold with one of the other condition types.

Syntax

```
>>-UPDate STAtusthreshold--threshold_name--+-----------------------------+-->
                                           '-Activity--=--activity_name-'

>--+-------------------------+--+-----------------+------------>
   '-Condition--=--+-EXists-+-'  '-Value--=--value-'
                   +-GT-----+
                   +-GE-----+
                   +-LT-----+
                   +-LE-----+
                   '-EQual--'

>--+-----------------------+---------------------------------><
   '-STatus--=--+-Normal--+-'
                +-Warning-+
                '-Error---'
```

Parameters

threshold_name (Required)
: Specifies the threshold name that you want to update. The name cannot exceed 48 characters in length.

activity
: Specify this value to change the activity for an existing threshold. This parameter is optional. Specify one of the following values:

  PROCESSSUMMARY
  : Specifies the number of processes that are currently active.

  SESSIONSUMMARY
  : Specifies the number of sessions that are currently active.

  CLIENTSESSIONSUMMARY
  : Specifies the number of client sessions that are currently active.

  SCHEDCLIENTSESSIONSUMMARY
  : Specifies the number of scheduled client sessions.

  DBUTIL
  : Specifies the database utilization percentage. The default warning threshold value is 80%, and the default error threshold value is 90%.

DBFREESPACE
: Specifies the free space available in the database in gigabytes.

DBUSEDSPACE
: Specifies the amount of database space that is used, in gigabytes.

ARCHIVELOGFREESPACE
: Specifies the free space that is available in the archive log, in gigabytes.

STGPOOLUTIL
: Specifies the storage pool utilization percentage. The default warning threshold value is 80%, and the default error threshold value is 90%.

STGPOOLCAPACITY
: Specifies the storage pool capacity in gigabytes.

AVGSTGPOOLUTIL
: Specifies the average storage pool utilization percentage across all storage pools. The default warning threshold value is 80%, and the default error threshold value is 90%.

TOTSTGPOOLCAPACITY
: Specifies the total storage pool capacity in gigabytes for all available storage pools.

TOTSTGPOOLS
: Specifies the number of defined storage pools.

TOTRWSTGPOOLS
: Specifies the number of defined storage pools that are readable or writeable.

TOTNOTRWSTGPOOLS
: Specifies the number of defined storage pools that are not readable or writeable.

STGPOOLINUSEANDDEFINED
: Specifies the total number of defined volumes that are in use.

ACTIVELOGUTIL
: Specifies the current percent utilization of the active log. The default warning threshold value is 80%, and the default error threshold value is 90%.

ARCHLOGUTIL
: Specifies the current utilization of the archive log. The default warning threshold value is 80%, and the default error threshold value is 90%.

CPYSTGPOOLUTIL
: Specifies the percent utilization for a copy storage pool. The default warning threshold value is 80%, and the default error threshold value is 90%.

PMRYSTGPOOLUTIL
: Specifies the percent utilization for a primary storage pool. The default warning threshold value is 80%, and the default error threshold value is 90%.

DEVCLASSPCTDRVOFFLINE
: Specifies the percent utilization of drives that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDRVPOLLING
: Specifies the drives polling, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTLIBPATHSOFFLINE
: Specifies the library paths that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTPATHSOFFLINE
: Specifies the percentage of device class paths that are offline, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDISKSNOTRW
: Specifies the percentage of disks that are not writable for the disk device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

DEVCLASSPCTDISKSUNAVAILABLE
: Specifies the percentage of the disk volumes that are unavailable, by device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

FILEDEVCLASSPCTSCRUNALLOCATABLE
: Specifies the percentage of scratch volumes that the server cannot allocate for a given non-shared file device class. The default warning threshold value is 25%, and the default error threshold value is 50%.

Condition
: Specify this value to change the condition of an existing threshold. This parameter is optional. Specify one of the following values:

EXists
: Creates a status monitoring indicator if the activity exists.

GT
: Creates a status monitoring indicator if the activity outcome is greater than the specified value.

GE
: Creates a status monitoring indicator if the activity outcome is greater than or equal to the specified value.

LT
: Creates a status monitoring indicator if the activity outcome is less than the specified value.

LE
: Creates a status monitoring indicator if the activity outcome is less than or equal to the specified value.

EQual
: Creates a status monitoring indicator if the activity outcome is equal to the specified value.

Value
: Specify this parameter to change the value that is compared with the activity output for the specified condition. You can specify an integer in the range 0 - 999999999999999.

STatus
: Specify this value to change the status of the indicator that is created in status monitoring if the condition that is being evaluated passes. This parameter is optional. Specify one of the following values:

  Normal
  : Specifies that the status indicator has a normal status value.

  Warning
  : Specifies that the status indicator has a warning status value.

  Error
  : Specifies that the status indicator has an error status value.

Update an existing status threshold

Update a status threshold for average storage pool utility percentage by issuing the following command:

```
update statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=90 condition=gt status=error
```

Related commands

Table 1. Commands related to UPDATE STATUSTHRESHOLD

Command	Description
DELETE STATUSTHRESHOLD (Delete a status monitoring threshold)	Deletes a status monitoring threshold.
QUERY MONITORSTATUS (Query the monitoring status)	Displays information about monitoring alerts and server status settings.
QUERY MONITORSETTINGS (Query the configuration settings for monitoring alerts and server status)	Displays information about monitoring alerts and server status settings.
QUERY STATUSTHRESHOLD (Query status monitoring thresholds)	Displays information about a status monitoring thresholds.
SET STATUSMONITOR (Specifies whether to enable status monitoring)	Specifies whether to enable status monitoring.
SET STATUSATRISKINTERVAL (Specifies whether to enable client at-risk activity interval evaluation)	Specifies whether to enable client at-risk activity interval evaluation
SET STATUSREFRESHINTERVAL (Set refresh interval for status monitoring)	Specifies the refresh interval for status monitoring.
SET STATUSSKIPASFAILURE (Specifies whether to use client at-risk skipped files as failure evaluation)	Specifies whether to use client at-risk skipped files as failure evaluation
UPDATE STATUSTHRESHOLD (Update a status monitoring threshold)	Changes the attributes of an existing status monitoring threshold.

UPDATE STGPOOL (Update a storage pool)

Use this command to change a storage pool.

Restriction: If a client is using the simultaneous-write function and data deduplication, the data deduplication feature is disabled during backups to a storage pool.

The UPDATE STGPOOL command takes seven forms. The syntax and parameters for each form are defined separately.

Table 1. Commands related to UPDATE STGPOOL

Command	Description
BACKUP STGPOOL	Backs up a primary storage pool to a copy storage pool.
COPY ACTIVEDATA	Copies active backup data.
DEFINE COLLOCGROUP	Defines a collocation group.
DEFINE COLLOCMEMBER	Adds a client node or file space to a collocation group.
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DELETE COLLOCGROUP	Deletes a collocation group.
DELETE COLLOCMEMBER	Deletes a client node or file space from a collocation group.
DELETE STGPOOL	Deletes a storage pool from server storage.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
MOVE MEDIA	Moves storage pool volumes that are managed by an automated library.
QUERY COLLOCGROUP	Displays information about collocation groups.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY NODEDATA	Displays information about the location and size of data for a client node.
QUERY SHREDSTATUS	Displays information about data waiting to be shredded.
QUERY STGPOOL	Displays information about storage pools.
RESTORE STGPOOL	Restores files to a primary storage pool from copy storage pools.
RESTORE VOLUME	Restores files stored on specified volumes in a primary storage pool from copy storage pools.
SET DRMDBBACKUPEXPIREDAYS	Specifies criteria for database backup series expiration.
SHRED DATA	Manually starts the process of shredding deleted data.
UPDATE COLLOCGROUP	Updates the description of a collocation group.

- UPDATE STGPOOL (Update a cloud-container storage pool)
  Use this command to update a container storage pool in a cloud environment. Cloud storage pools are not supported on Linux on System z®.
- UPDATE STGPOOL (Update a directory-container storage pool)
  Use this command to update a directory-container storage pool.
- UPDATE STGPOOL (Update a container-copy storage pool)
  Use this command to update a container-copy storage pool.
- UPDATE STGPOOL (Update a primary random access storage pool)
  Use this command to update a random access storage pool.
- UPDATE STGPOOL (Update a primary sequential access pool)
  Use this command to update a primary sequential access storage pool.
- UPDATE STGPOOL (Update a copy sequential access storage pool)
  Use this command to update a copy sequential access storage pool.
- UPDATE STGPOOL (Update an active-data sequential access)
  Use this command to update an active-data pool.

UPDATE STGPOOL (Update a cloud-container storage pool)

Use this command to update a container storage pool in a cloud environment. Cloud storage pools are not supported on Linux on System z®.

The preferred way to define and configure a cloud-container storage pool is to use the Operations Center. For instructions and tips for the Operations Center and the command-line interface, see Configuring a cloud-container storage pool for data storage.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax

```
>>-UPDate STGpool--pool_name--+-----------------------------+--->
                              '-DESCription--=--description-'

>--+-------------------------------------+----------------------->
   |                                 (1) |
   '-CLOUDType--=--+-SWift---------+-----'
                   +-IBMCLoudswift-+
                   '-V1Swift-------'

>--+-------------------------+----------------------------------->
   '-CLOUDUrl--=--cloud_url-'

>--+---------------------------------+-------------------------->
   |                             (2) |
   '-IDentity--=--cloud_identity-----'

>--+-----------------------+----------------------------------->
   '-PAssword--=--password-'

>--+---------------------------------+-------------------------->
   '-CLOUDLocation--=--+-OFfpremise-+-'
                       '-ONpremise--'

>--+---------------------------------+-------------------------->
   |                             (3) |
   '-BUCKETName--=--bucket_name-----'

>--+-----------------------------+------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                +-UNAVailable-+
                '-DESTroyed---'

>--+-------------------------------------+----------------------->
   '-MAXWriters--=--+-NOLimit---------+-'
                    '-maximum_writers-'

>--+---------------------+------------------------------------->
   '-REUsedelay--=--days-'

>--+-----------------------------------------------------+-------><
   |                       .-COMPRession--=--Yes-----. |
   '-ENCRypt--=--+-Yes-+--+-------------------------+-'
                 '-No--'  '-COMPRession--=--+-Yes-+-'
                                            '-No--'
```

Notes:

1. CLOUDTYPE=S3 and CLOUDTYPE=AZURE cannot be changed.
2. For Azure storage pools, it is not necessary to specify the IDENTITY parameter.
3. This parameter is valid only if you specify CLOUDTYPE=S3.

Parameters

pool_name (Required)
Specifies the storage pool to update. This parameter is required.

DESCription
Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains blank characters. To remove an existing description, specify a null string ("").

CLOUDType
Specifies the type of cloud environment where you are configuring a storage pool. This parameter is optional. Specify one of the following values:

IBMCLoudswift
Specifies that the storage pool uses an IBM® Cloud cloud computing system with an OpenStack Swift cloud computing system.

SWift
Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 2 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol it is using.

V1Swift
Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 1 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol it is using.

Restriction: If you used the DEFINE STGPOOL command to define a storage pool with CLOUDTYPE=S3 (Simple Storage Service) or CLOUDTYPE=AZURE, you cannot change to a different cloud type by using the UPDATE STGPOOL command. Additionally, you cannot change the following cloud types by using the UPDATE STGPOOL command:

- A non-S3 storage pool to S3
- A non-Azure storage pool to Azure

CLOUDUrl
Specifies the URL of the cloud environment where you are configuring the storage pool. Based on your cloud provider, you can use a region endpoint URL, an accesser IP address, a public authentication endpoint, or a similar value for this parameter. Be sure to include the protocol, such as `https://` or `http://`, at the beginning of the URL. The maximum length of the web address is 870 characters. The CLOUDURL parameter is not validated until the first backup begins.
For more information about how to locate these values, select your cloud service provider from the list on the Configuring a cloud-container storage pool for data storage page.
Tip: To use more than one IBM Cloud Object Storage accesser, list the accesser IP addresses separated by a vertical bar (|), with no spaces, such as in the following example:

```
CLOUDURL=<accesser_URL1>|<accesser_URL2>|<accesser_URL3>
```

Use multiple accessers to improve performance. If you are using the IBM Cloud S3 solution, only one accesser is needed.

IDentity
Specifies the user ID for the cloud that is specified in the STGTYPE=CLOUD parameter. This parameter is required for all supported cloud computing systems except Azure. If you specified CLOUDTYPE=AZURE, do not specify the IDENTITY parameter. Based on your cloud provider, you can use an access key ID, a user name, a tenant name and user name, or a similar value for this parameter. The maximum length of the user ID is 255 characters.

PAssword (Required)
Specifies the password for the cloud that is specified in the STGTYPE=CLOUD parameter. Based on your cloud provider, you can use a shared access signature (SAS) token, secret access key, an API key, a password, or a similar value for this parameter. This parameter is required. The maximum length of the password is 255 characters. The IDENTITY and PASSWORD parameters are not validated until the first backup begins.

CLOUDLocation
Specifies the physical location of the cloud that is specified in the CLOUD parameter. This parameter is optional. You can specify one of the following values:

- OFfpremise
- ONpremise

BUCKETName
Specifies the name for an Amazon Web Services (AWS) bucket or IBM Cloud Object Storage vault to use with this storage pool. AWS buckets and IBM Cloud Object Storage vaults are used in the same manner as containers in a cloud-container storage pool. This parameter is optional, and is valid only if this storage pool has a cloud type of S3. If the name that you specify does not exist, the server creates a bucket or vault with the specified name before using the bucket or vault. Follow

the naming restrictions for your cloud provider when specifying this parameter. Review the permissions for the bucket or vault and ensure that the credentials for this storage pool have permission to read, write, list, and delete objects in this bucket or vault.

Restriction: You cannot change the bucket or vault if any cloud containers exist in this storage pool.

ACCess

Specifies how client nodes and server processes access the storage pool. This parameter is optional. You can specify one of the following values:

READWrite
: Specifies that client nodes and server processes can read and write to the storage pool.

READOnly
: Specifies that client nodes and server processes can read only from the storage pool.

UNAVailable
: Specifies that client nodes and server processes cannot access the storage pool. As a result, backups and restore fail for this storage pool. You can use this value to specify that the cloud service provider is temporarily unavailable.

DESTroyed
: Specifies that client nodes and server processes cannot access the storage pool because the cloud service provider is permanently unavailable. Backups and restores fail for this storage pool, but any attempts to delete objects and containers from this storage pool finish successfully.

MAXWriters

Specifies the maximum number of writing sessions that can run concurrently on the storage pool. Specify a maximum number of writing sessions to control the performance of the cloud storage pool from negatively impacting other system resources. This parameter is optional. You can specify one of the following values:

NOLimit
: Specifies that no maximum size limit exists for the number of writers that you can use. This value is the default.

maximum_writers
: Limits the maximum number of writers that you can use. Specify an integer in the range 1 - 99999.

REUsedelay

Specifies the number of days that must elapse after all deduplicated extents are removed from a cloud storage pool. This parameter controls the duration that deduplicated extents are associated with a cloud storage pool. When the value that is specified for the parameter expires, the deduplicated extents are deleted from the cloud storage pool. This parameter is optional. You can specify one of the following values:

1
: Specifies that deduplicated extents are deleted from a cloud storage pool after one day.

days
: You can specify an integer in the range 0 - 9999.

Tip: Set this parameter to a value that is greater than the number specified for the SET DRMDBBACKUPEXPIREDAYS command. By setting this parameter to a higher value, you can ensure that when you restore the database to an earlier level, the references to files in the storage pool are still valid.

ENCRypt

Specifies whether the server encrypts client data before it writes it to the storage pool. You can specify the following values:

Yes
: Specifies that client data is encrypted by the server.

No
: Specifies that client data is not encrypted by the server.

This parameter is optional. The default depends on the physical location of the cloud, which is specified by the CLOUDLOCATION parameter. If the cloud is off premise, the server encrypts data by default. If the cloud is on premises, the server does not encrypt data by default.

COMPRession

Specifies whether data is compressed in the storage pool. This parameter is optional. You can specify one of the following values:

No
: Specifies that data is not compressed in the storage pool.

Yes

Specifies that data is compressed in the storage pool. This is the default.

Example 1: Update a cloud storage pool to specify a maximum number of data sessions

Update a cloud storage pool that is named STGPOOL1 and specify a maximum of 10 data sessions.

```
update stgpool stgpool1 maxwriters=10
```

Example 2: Update the description of a cloud-container storage pool

Update a cloud-container storage pool that is named STGPOOL2. Remove the existing description from the storage pool.

```
update stgpool stgpool2 cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 description=""
```

Related tasks:
Configuring a cloud-container storage pool for data storage
AIX Linux Windows

UPDATE STGPOOL (Update a directory-container storage pool)

Use this command to update a directory-container storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax

```
'-No--'
```

Parameters

pool_name (Required)
: Specifies the storage pool to update. This parameter is required. The maximum length of the name is 30 characters.

DESCription
: Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
: Specifies how client nodes and server processes access files in the storage pool. This parameter is optional. You can specify one of the following values:

  READWrite
  : Specifies that client nodes and server processes can read and write to the storage pool. This is the default.

  READOnly
  : Specifies that client nodes and server processes can only read from the storage pool.

  UNAVailable
  : Specifies that client nodes and server processes cannot access the storage pool.

MAXSIze
: Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. The default value is NOLIMIT. Specify one of the following values:

  NOLimit
  : Specifies that there is no maximum size limit for physical files that are stored in the storage pool.

  maximum_file_size
  : Limits the maximum physical file size. Specify an integer in the range 1 - 999999, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 GB. Use one of the following scale factors:

    Table 1. Scale factor for the maximum file size

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

    Tip: If you do not specify a unit of measurement for the maximum file size, the value is specified in bytes.

  When the physical size of the storage pool exceeds the MAXSIZE parameter, the following table shows where files are typically stored.

Table 2. The location of a file according to the file size and the pool that is specified

Pool that is specified	Result
No pool is specified as the next storage pool in the hierarchy.	The server does not store the file.
A pool is specified as the next storage pool in the hierarchy.	The server stores the file in the storage pool that you specified.

Tip: If you also specify the NEXTstgpool parameter, update one storage pool in your hierarchy to have no limit on the maximum file size by specifying the MAXSIze=NOLimit parameter. When you have at least one pool with no size limit, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent during data deduplication processing, the server considers the size of the data deduplication process to be the file size. If the total size of all files in the process is larger than the maximum size limit, the server does not store the files in the storage pool.

MAXWriters
Specifies the maximum number of I/O threads that can run concurrently on the storage pool. Specify a maximum number of I/O threads to control the number of I/O threads that are written simultaneously to the directory-container storage pool. This parameter is optional. As a best practice, use the default value of NOLIMIT. You can specify one of the following values:

NOLimit
Specifies that no maximum number of I/O threads are written to the storage pool.
maximum_writers
Limits the maximum number of I/O threads that you can use. Specify an integer in the range 1 - 99999.

NEXTstgpool
Specifies the name of a random-access or primary sequential storage pool to which files are stored when the directory-container storage pool is full. This parameter is optional.
Restrictions:

- To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.
- If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
- Do not specify a directory-container or cloud-container storage pool.
- Do not use this parameter to specify a storage pool for data migration.

PROTECTstgpool
Specifies the name of the directory-container storage pool on the target server where the data is backed up when you use the PROTECT STGPOOL command for this storage pool. This parameter is optional.
PROTECTLOCalstgpools
Specifies the name of the container-copy storage pool on a local device where the data is backed up. This container-copy storage pool will be a local target storage pool when you use the PROTECT STGPOOL command. You can specify a maximum of two container-copy storage pool names to update. Separate multiple names with commas and no intervening spaces. The maximum length of each name is 30 characters. This parameter is optional.
To add or remove container-copy storage pools, specify the container-copy storage pool names to include. For example, if the existing container-copy storage pool includes COPY1 and you want to add COPY2, specify PROTECTLOCALSTGPOOLS=COPY1,COPY2. To remove all existing container-copy storage pools that are associated with the primary storage pool, specify a null string (""). For example, COPYSTGPOOLS="".
REUsedelay
Specifies the number of days that must elapse before all deduplicated extents are removed from a directory-container storage pool. This parameter controls the duration that deduplicated extents are associated with a directory-container storage pool. When the value that is specified for the parameter expires, the deduplicated extents are deleted from the directory-container storage pool. The default is 1. Specify one of the following values:

days
Specify an integer in the range 0 - 9999.
1
Specifies that deduplicated extents are deleted from a directory-container storage pool after one day.

Tip: Set this parameter to a value greater than the number that is specified as your database backup period to ensure that data extents are still valid when you restore the database to another level.
ENCRypt
Specifies whether the server encrypts client data before the server writes the data to the storage pool. You can specify the following values:

Yes
Specifies that client data is encrypted by the server.
No
Specifies that client data is not encrypted by the server.

COMPRession
Specifies whether data is compressed in the storage pool. This parameter is optional. You can specify one of the following values:

No
Specifies that data is not compressed in the storage pool.
Yes

Specifies that data is compressed in the storage pool. This is the default.

Example: Update a storage pool to specify a maximum number of data sessions

Update a storage pool that is named STGPOOL1 and specify a maximum of 10 data sessions.

```
update stgpool stgpool1 maxwriters=10
```

Example: Update a storage pool to specify the maximum size

Update a storage pool that is named STGPOOL2. The storage pool specifies the maximum file size that the server can store in the storage pool as 100 megabytes.

```
update stgpool stgpool2 maxsize=100M
```

Example: Update the description of a storage pool

Update a storage pool that is named STGPOOL3. Remove the existing description from the storage pool.

```
update stgpool stgpool3 description=""
```

Table 3. Commands related to UPDATE STGPOOL

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
QUERY CONTAINER	Displays information about a container.
QUERY STGPOOL	Displays information about storage pools.
REPAIR STGPOOL	Repairs a directory-container storage pool.
AIX Linux Windows UPDATE STGPOOLDIRECTORY	Changes the attributes of a storage pool directory.

UPDATE STGPOOL (Update a container-copy storage pool)

Use this command to update a container-copy storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to be updated.

Syntax

```
>>-UPDate STGpool--pool_name--+-----------------------+--------->
                              '-MAXSCRatch--=--number-'

>--+-----------------------------+----------------------------->
   '-DESCription--=--description-'

>--+-----------------------------+----------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

>--+---------------------------+--+--------------------+------->
   '-PROTECTPRocess--=--number-'  '-RECLaim--=--percent-'

>--+-------------------------------+--------------------------->
```

```
   '-RECLAIMLIMit--=--+-NOLimit---+-'
                      '-vol_limit-'

>--+--------------------+-----------------------------------><
   '-REUsedelay--=--days-'
```

Parameters

pool_name (Required)
: Specifies the name of the storage pool to be updated.

MAXSCRatch
: Specifies the maximum number of scratch volumes that the server can request for this storage pool. You can specify an integer in the range 0 - 100000000. If the server can request scratch volumes as needed, you do not have to define each volume to be used.

  The value of this parameter is used to estimate the total number of volumes that are available in the storage pool and the corresponding estimated capacity for the storage pool.

DESCription
: Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
: Specifies how server processes such as storage-pool protection and repair can access data in the storage pool. This parameter is optional. You can specify one of the following values:

  READWrite
  : Specifies that the server can read and write to volumes in the storage pool.

  READOnly
  : Specifies that the server can only read volumes in the storage pool. The server can use data in the storage pool to restore extents to directory-container storage pools. No operations that write to the container-copy storage pool are allowed.

  UNAVailable
  : Specifies that the server cannot access data that is stored on volumes in the storage pool.

PROTECTPRocess
: Specifies the maximum number of parallel processes that are used when you issue the PROTECT STGPOOL command to copy data to this pool from a directory-container storage pool. This parameter is optional. Enter a value in the range 1 - 20.

  The time that is required to complete the copy operation might be decreased by using multiple, parallel processes. However, in some cases when multiple processes are running, one or more of the processes must wait to use a volume that is already in use by a different process.

  When you select this value, consider the number of logical and physical drives that can be dedicated to this operation. To access a tape volume, the server uses a mount point and a drive. The number of available mount points and drives depends on the mount limit of the device class for the storage pool, and on other server and system activity.

  If you use the preview option on the PROTECT STGPOOL command, only one process is used and no mount points or drives are needed.

RECLaim
: Specifies when a volume becomes eligible for reclamation and reuse. Specify eligibility as the percentage of a volume's space that is occupied by extents that are no longer stored in the associated directory-container storage pool. Reclamation moves any extents that are still stored in the associated directory-container storage pool from eligible volumes to other volumes. Reclamation occurs only when a PROTECT STGPOOL command stores data into this storage pool.

  This parameter is optional. You can specify an integer in the range 1 - 100. The value 100 specifies that volumes in this storage pool are not reclaimed.

  The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

  By setting the reclaim value to 50 percent or greater, data that is moved from two reclaimed volumes uses no more than the equivalent of one new volume.

Use caution when you use reclamation with container-copy storage pools that have offsite volumes. When an offsite volume becomes eligible for reclamation, in effect the server moves the extents on the volume back to the onsite location. If a disaster occurs onsite, the server can obtain extents from the offsite volume if the restored database refers to extents on the offsite volume. Therefore, for disaster recovery purposes, ensure that you schedule database backups to run after storage pool protection schedules and DRM move schedules have run, and ensure that all database backup volumes are taken offsite along with the DRM volumes.

Tip: Set different reclamation values for offsite container-copy storage pools and onsite container-copy storage pools. Because container-copy storage pools store deduplicated data, the data extents are spread across multiple tape volumes. When you choose a reclamation threshold for an offsite copy, carefully consider the number of available mount points and the number of tape volumes that you must retrieve if a disaster occurs. Setting a higher threshold means that you must retrieve more volumes than you would if your reclamation value was lower. Using a lower threshold reduces the number of mount points that are required in a disaster. The preferred method is to set the reclamation value for offsite copies to 60, and for onsite copies, in the range 90 - 100.

RECLAIMLIMit
Specifies the maximum number of volumes that the server reclaims when you issue the PROTECT STGPOOL command and specify the RECLAIM=YESLIMITED or RECLAIM=ONLYLIMITED option. This parameter is valid only for container-copy storage pools. This parameter is optional. You can specify one of the following values:

NOLimit
Specifies that all volumes in the container-copy storage pool are processed for reclamation.

vol_limit
Specifies the maximum number of volumes in the container-copy storage pool that are reclaimed. The value that you specify determines how many new scratch tapes are available after reclamation processing completes. You can specify a number in the range 1 - 100000.

REUsedelay
Specifies the number of days that must elapse after all extents are deleted from a volume before the volume can be rewritten or returned to scratch status. This parameter is optional. You can specify an integer in the range 0 - 9999. A value of 0 means that a volume can be rewritten or returned to scratch status as soon as all the extents are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to extents in the storage pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. If you use disaster recovery manager, the number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

Example: Update a container-copy storage pool to delay volume reuse for 30 days

Update the storage pool that is named CONTAINER1_COPY2 to change the delay for volume reuse to 30 days.

```
update stgpool container1_copy2 reusedelay=30
```

Example: Update a container-copy storage pool to limit the number of reclaimed tape volumes to 10

Update the storage pool that is named CONTAINER1_COPY2 to change the reclaim limit to 10 volumes.

```
update stgpool container1_copy2 reclaimlimit=10
```

Table 1. Commands related to UPDATE STGPOOL (Update a container-copy storage pool)

Command	Description
DEFINE STGPOOL (container-copy)	Define a container-copy storage pool that stores copies of data from a directory-container storage pool.
PROTECT STGPOOL	Protects a directory-container storage pool.
QUERY STGPOOL	Displays information about storage pools.
REPAIR STGPOOL	Repairs a directory-container storage pool.
UPDATE STGPOOL (directory-container)	Update a directory-container storage pool.

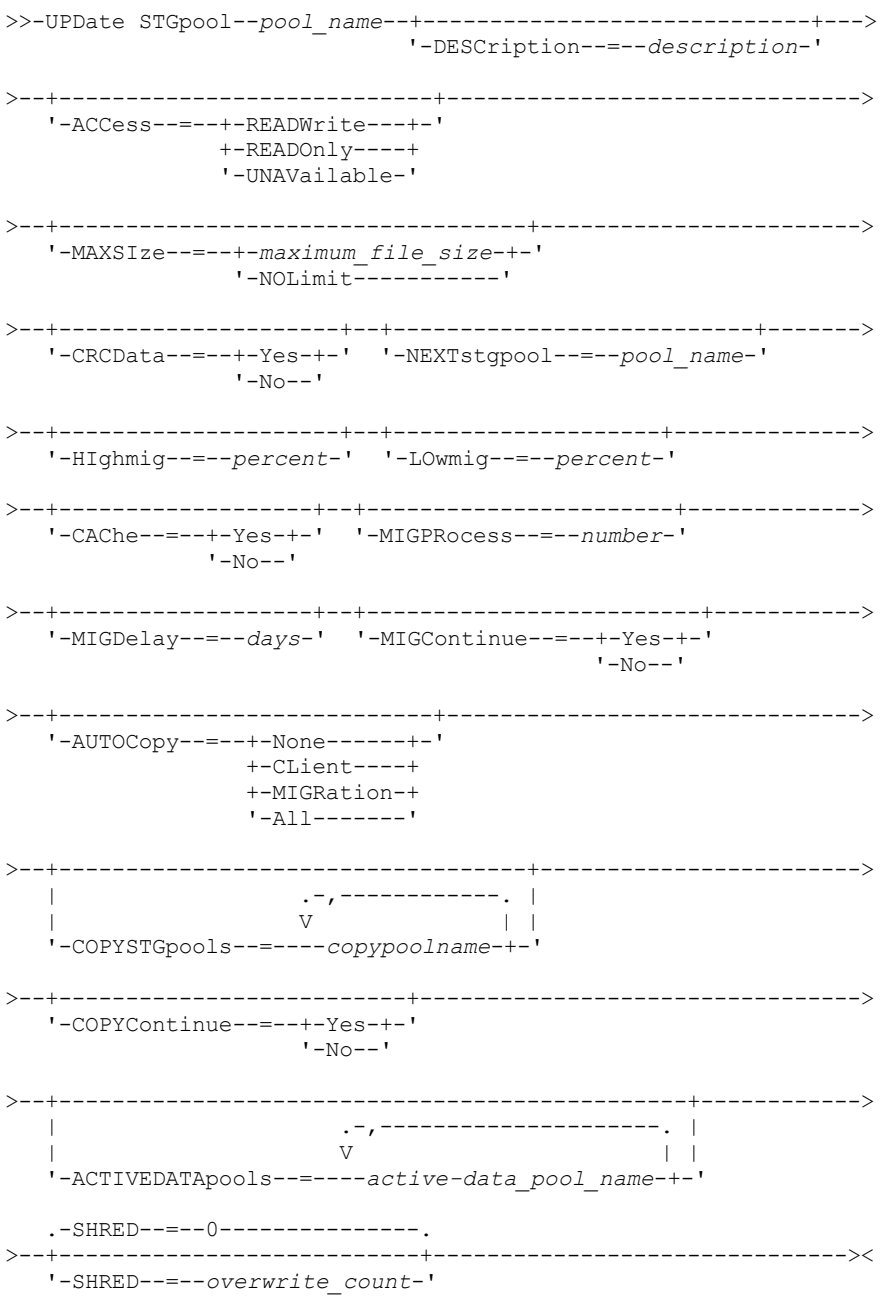
UPDATE STGPOOL (Update a primary random access storage pool)

Use this command to update a random access storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to be updated.

Syntax



Parameters

pool_name (Required)
: Specifies the storage pool to update. This parameter is required.

DESCription
: Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
Specifies how client nodes and server processes (such as migration and reclamation) can access files in the storage pool. This parameter is optional. You can specify the following values:

READWrite
Specifies that client nodes and server processes can read and write to files stored on volumes in the storage pool.

READOnly
Specifies that client nodes can only read files from the volumes in the storage pool.

Server processes can move files within the volumes in the storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *readonly*, the storage pool is skipped when server processes attempt to write files to the storage pool.

UNAVailable
Specifies that client nodes cannot access files stored on volumes in the storage pool.

Server processes can move files within the volumes in the storage pool and can also move or copy files from this storage pool to another storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *unavailable*, the storage pool is skipped when server processes attempt to write files to the storage pool.

MAXSIze
Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. You can specify the following values:

NOLimit
Specifies that there is no maximum size limit for physical files stored in the storage pool.

maximum_file_size
Limits the maximum physical file size. Specify an integer from 1 to 999999 terabytes, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 gigabytes. Scale factors are:

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

The client estimates the size of files that are sent to the server. The client estimate is used rather than the actual amount of data that is sent to the server. Client options, such as deduplication, compression, and encryption, can cause the actual amount of data that is sent to the server to be larger or smaller than the size estimate. For example, the compression of a file might be smaller in size than the estimate, thus sending less data than the estimate. Furthermore, a binary file might be larger in size after the compression processing, thus sending more data than the estimate.

See the following table for information about where a file is stored when its size exceeds the MAXSIZE parameter.

Table 1. Where a file is stored according to the file size and the pool that is specified

File size	Pool specified	Result
Exceeds the maximum size	No pool is specified as the next storage pool in the hierarchy	The server does not store the file
	A pool is specified as the next storage pool in the hierarchy	The server stores the file in the next storage pool that can accept the file size

If you specify the next storage pool parameter, define one storage pool in your hierarchy to have no limit on the maximum file size. By having no limit on the size for at least one pool, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent in a single transaction, the server considers the size of the transaction to be the file size. If the total size of all files in the transaction is larger than the maximum size limit, the server does not store the files in the

storage pool.

CRCData
: Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

  Yes
  : Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more expenditure is required to calculate and compare CRC values between the storage pool and the server.

  No
  : Specifies that data is stored without CRC information.

NEXTstgpool
: Specifies a primary storage pool to which files are migrated. This parameter is optional.

  To remove an existing storage pool from the storage hierarchy, specify a null string ("") for this value.

  If you do not specify a next storage pool, the following actions occur:

  - The server cannot migrate files from this storage pool
  - The server cannot store files that exceed the maximum size for this storage pool in another storage pool

  Restrictions:

  - To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.
  - If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
  - Do not specify a directory-container or cloud-container storage pool.
  - Do not use this parameter to specify a storage pool for data migration.

HIghmig
: Specifies that the server starts migration for this storage pool when the amount of data in the pool reaches this percentage of the pool's estimated capacity. This parameter is optional. You can specify an integer 0 - 100.

  When the storage pool exceeds the high migration threshold, the server can start migration of files by node to the next storage pool, as defined with the NEXTSTGPOOL parameter. You can specify HIGHMIG=100 to prevent migration for this storage pool.

LOwmig
: Specifies that the server stops migration for this storage pool when the amount of data in the pool reaches this percentage of the pool's estimated capacity. You can specify an integer 0 - 99 for this optional parameter.

  When migration is by node or file space, depending upon collocation, the level of the storage pool can fall below the value that you specified for this parameter. To empty the storage pool, set LOWMIG=0.

CAChe
: Specifies whether the migration process leaves a cached copy of a file in this storage pool after you migrate the file to the next storage pool. This parameter is optional. You can specify the following values:

  Yes
  : Specifies that caching is enabled.

  No
  : Specifies that caching is disabled.

  Using cache might improve your ability to retrieve files, but might affect the performance of other processes.

MIGPRocess
: Specifies the number of processes that are used for migrating files from this storage pool. This parameter is optional. You can specify an integer 1 - 999.

  During migration, these processes are run in parallel to provide the potential for improved migration rates.

Tips:

- The number of migration processes is dependent upon the following settings:
  - The setting of the MIGPROCESS parameter
  - The collocation setting of the next pool
  - The number of nodes or the number of collocation groups with data in the storage pool that is being migrated

  For this example, `MIGPROCESS =6`, the next pool COLLOCATE parameter is NODE, but there are only two nodes with data on the storage pool. Migration processing consists of only two processes, not six. If the COLLOCATE parameter is GROUP group and both nodes are in the same group, migration processing consists of only one process. If the COLLOCATE parameter is NO or FILESPACE group, and each node has two file spaces with backup data, then migration processing consists of only four processes.
- When you specify this parameter, consider whether the simultaneous-write function is enabled for server data migration. Each migration process requires a mount point and a drive for each copy storage pool and active-data pool that is defined to the target storage pool.

MIGDelay
: Specifies the minimum number of days a file must remain in a storage pool before it becomes eligible for migration. To calculate a value to compare to the specified MIGDELAY value, the server counts the following items:

  - The number of days that the file was in the storage pool
  - The number of days, if any, since the file was retrieved by a client

  The lesser of the two values are compared to the specified MIGDELAY value. For example, if all the following conditions are true, a file is not migrated:

  - A file was in a storage pool for five days.
  - The file was accessed by a client within the past three days.
  - The value that is specified for the MIGDELAY parameter is four days.

  This parameter is optional. You can specify an integer 0 - 9999. The default is 0, which means that you do not want to delay migration.

  If you want the server to count the number of days that are based on when a file was stored and not when it was retrieved, use the NORETRIEVEDATE server option.

MIGContinue
: Specifies whether you allow the server to migrate files that do not satisfy the migration delay time. This parameter is optional.

  Because you can require that files remain in the storage pool for a minimum number of days, the server may migrate all eligible files to the next storage pool yet not meet the low migration threshold. This parameter allows you to specify whether the server is allowed to continue the migration process by migrating files that do not satisfy the migration delay time.

  You can specify one of the following values:

  Yes
  : Specifies that, when necessary to meet the low migration threshold, the server continues to migrate files that do not satisfy the migration delay time.

    If you allow more than one migration process for the storage pool, some files that do not satisfy the migration delay time may be migrated unnecessarily. As one process migrates files that satisfy the migration delay time, a second process could begin migrating files that do not satisfy the migration delay time to meet the low migration threshold. The first process that is still migrating files that satisfy the migration delay time might have, by itself, caused the low migration threshold to be met.

  No
  : Specifies that the server stops migration when no eligible files remain to be migrated, even before reaching the low migration threshold. The server does not migrate files unless the files satisfy the migration delay time.

AUTOCopy
: Specifies when IBM Spectrum Protect™ runs simultaneous-write operations to copy storage pools and active-data pools. This parameter affects the following operations:

  - Client store sessions
  - Server import processes

- Server data-migration processes

If an error occurs while data is being simultaneously written to a copy storage pool or active-data pool during a migration process, the server stops writing to the failing storage pools for the remainder of the process. However, the server continues to store files into the primary storage pool and any remaining copy storage pools or active-data pools. These pools remain active for the duration of the migration process. Copy storage pools are specified using the COPYSTGPOOLS parameter. Active-data pools are specified using the ACTIVEDATAPOOLS parameter.

You can specify one of the following values:

None
: Specifies that the simultaneous-write function is disabled.

CLient
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions or server import processes. During server import processes, data is written simultaneously to only copy storage pools. Data is not written to active-data pools during server import processes.

MIGRation
: Specifies that data is written simultaneously to copy storage pools and active-data pools only during migration to this storage pool. During server data-migration processes, data is written simultaneously to copy storage pools and active-data pools only if the data does not exist in those pools. Nodes whose data is being migrated must be in a domain associated with an active-data pool. If the nodes are not in a domain associated with an active pool, the data cannot be written to the pool.

All
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions, server import processes, or server data-migration processes. Specifying this value ensures that data is written simultaneously whenever this pool is a target for any of the eligible operations.

COPYSTGpools
: Specifies the names of copy storage pools where the server simultaneously writes data. You can specify a maximum of three copy pool names that are separated by commas. Spaces between the names of the copy pools are not allowed. To add or remove one or more copy storage pools, specify the pool name or names that you want to include in the updated list. For example, if the existing copy pool list includes COPY1 and COPY2 and you want to add COPY3, specify COPYSTGPOOLS=COPY1,COPY2,COPY3. To remove all existing copy storage pools that are associated with the primary storage pool, specify a null string ("") for the value (for example, COPYSTGPOOLS="").

  When you specify a value for the COPYSTGPOOLS parameter, you can also specify a value for the COPYCONTINUE parameter. For more information, see the COPYCONTINUE parameter.

  The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

  When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of copy storage pools and the COPYCONTINUE value from the primary storage pool. The primary storage pool is specified by the copy group of the management class that is bound to the data.

  The server can write data simultaneously to copy storage pools for the following operations:

  - Back up and archive operations by IBM Spectrum Protect backup-archive clients or application clients that are using the IBM Spectrum Protect API
  - Migration operations by IBM Spectrum Protect for Space Management clients
  - Import operations that involve copying exported file data from external media to a primary storage pool associated with a copy storage pool list

  Restrictions: The simultaneous-write function is not supported for the following store operations:

  - When the operation is using LAN-free data movement. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is accepted.
  - NAS backup operations. If the primary storage pool specified in the DESTINATION or TOCDESTINATION in the copy group of the management class has copy storage pools that are defined:
    - The copy storage pools are ignored
    - The data is stored into the primary storage pool only

  Attention: The function that is provided by the COPYSTGPOOLS parameter is not intended to replace the BACKUP STGPOOL command. If you use the COPYSTGPOOLS parameter, continue to use the BACKUP STGPOOL command to ensure that the

copy storage pools are complete copies of the primary storage pool. There are cases when a copy might not be created. For more information, see the COPYCONTINUE parameter description.

COPYContinue

Specifies how the server reacts to a copy storage pool write failure for any of the copy storage pools that are listed in the COPYSTGPOOLS parameter. This parameter is optional. When you specify the COPYCONTINUE parameter, either a COPYSTGPOOLS list must exist or the COPYSTGPOOLS parameter must also be specified.
You can specify the following values:

Yes

If the COPYCONTINUE parameter is set to YES, the server will stop writing to the failing copy pools for the remainder of the session, but continue storing files into the primary pool and any remaining copy pools. The copy storage pool list is active only for the life of the client session and applies to all the primary storage pools in a particular storage pool hierarchy.

No

If the COPYCONTINUE parameter is set to NO, the server will fail the current transaction and discontinue the store operation.

Restrictions:

- The setting of the COPYCONTINUE parameter does not affect active-data pools. If a write failure occurs for any of the active-data pools, the server stops writing to the failing active-data pool for the remainder of the session, but continues storing files into the primary pool and any remaining active-data pools and copy storage pools. The active-data pool list is active only for the life of the session and applies to all the primary storage pools in a particular storage pool hierarchy.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server import. If data is being written simultaneously and a write failure occurs to the primary storage pool or any copy storage pool, the server import process fails.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server data migration. If data is being written simultaneously and a write failure occurs to any copy storage pool or active-data pool, the failing storage pool is removed and the data migration process continues. Write failures to the primary storage pool cause the migration process to fail.

ACTIVEDATApools

Specifies the names of active-data pools where the server simultaneously writes data during a client backup operation. The ACTIVEDATAPOOLS parameter is optional. Spaces between the names of the active-data pools are not allowed.

The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of active-data pools from the destination storage pool that is specified in the copy group. The primary storage pool is specified by the copy group of the management class that is bound to the data.

The server can write data simultaneously to active-data pools only during backup operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API.
Restrictions:

1. This parameter is available only to primary storage pools that use "NATIVE" or "NONBLOCK" data format. This parameter is not available for storage pools that use the following data formats:
    - NETAPPDUMP
    - CELERRADUMP
    - NDMPDUMP
2. Writing data simultaneously to active-data pools is not supported when you use LAN-free data movement. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is followed.
3. The simultaneous-write function is not supported when a NAS backup operation is writing a TOC file. If the primary storage pool specified in the TOCDESTINATION in the copy group of the management class has active-data pools that are defined:
    - The active-data pools are ignored
    - The data is stored into the primary storage pool only
4. You cannot use the simultaneous-write function with CENTERA storage devices.
5. Data that is being imported is not stored in active-data pools. After an import operation, use the COPY ACTIVEDATA command to store the imported data in an active-data pool.

Attention: The function that is provided by the ACTIVEDATAPOOLS parameter is not intended to replace the COPY ACTIVEDATA command. If you use the ACTIVEDATAPOOLS parameter, use the COPY ACTIVEDATA command to ensure that the active-data pools contain all active data of the primary storage pool.

SHRED

Specifies whether data is physically overwritten when it is deleted. This parameter is optional. You can specify an integer 0 - 10.

If you specify a value of zero, the server deletes the data from the database. However, the storage that is used to contain the data is not overwritten, and the data exists in storage until that storage is reused for other data. It might be possible to discover and reconstruct the data after it is deleted. Changing the value (for example, resetting it to 0) does not affect data that was deleted and is waiting to be overwritten.

If you specify a value greater than 0, the server deletes the data both logically and physically. The server overwrites the storage that is used to contain the data the specified number of times. This overwriting increases the difficulty of discovering and reconstructing the data after it is deleted.

To ensure that all copies of the data are shredded, specify a SHRED value greater than zero for the storage pool that is specified in the NEXTSTGPOOL parameter. Do not specify either the COPYSTGPOOLS or ACTIVEDATAPOOLS. Specifying relatively high values for the overwrite count generally improves the level of security, but might affect performance adversely.

Overwriting of deleted data is done asynchronously after the delete operation is complete. Therefore, the space that is occupied by the deleted data remains occupied for some time. The space is not available as free space for new data.

A SHRED value greater than zero cannot be used if the value of the CACHE parameter is YES. If you want to enable shredding for an existing storage pool for which caching is already enabled, you must change the value of the CACHE parameter to NO. Existing cached files remain in storage so that subsequent retrieval requests can be satisfied quickly. If space is needed to store new data, the existing cached files are erased so that the space they occupied can be used for the new data. The existing cached files are not shredded when they are erased.
Important: After an export operation finishes and identifies files for export, any change to the storage pool SHRED value is ignored. An export operation that is suspended retains the original SHRED value throughout the operation. You might want to consider canceling your export operation if changes to the storage pool SHRED value jeopardize the operation. You can reissue the export command after any needed cleanup.

Example: Update a random access storage pool to allow caching

Update the random access storage pool that is named BACKUPPOOL to allow caching when the server migrates files to the next storage pool.

```
update stgpool backuppool cache=yes
```

UPDATE STGPOOL (Update a primary sequential access pool)

Use this command to update a primary sequential access storage pool.

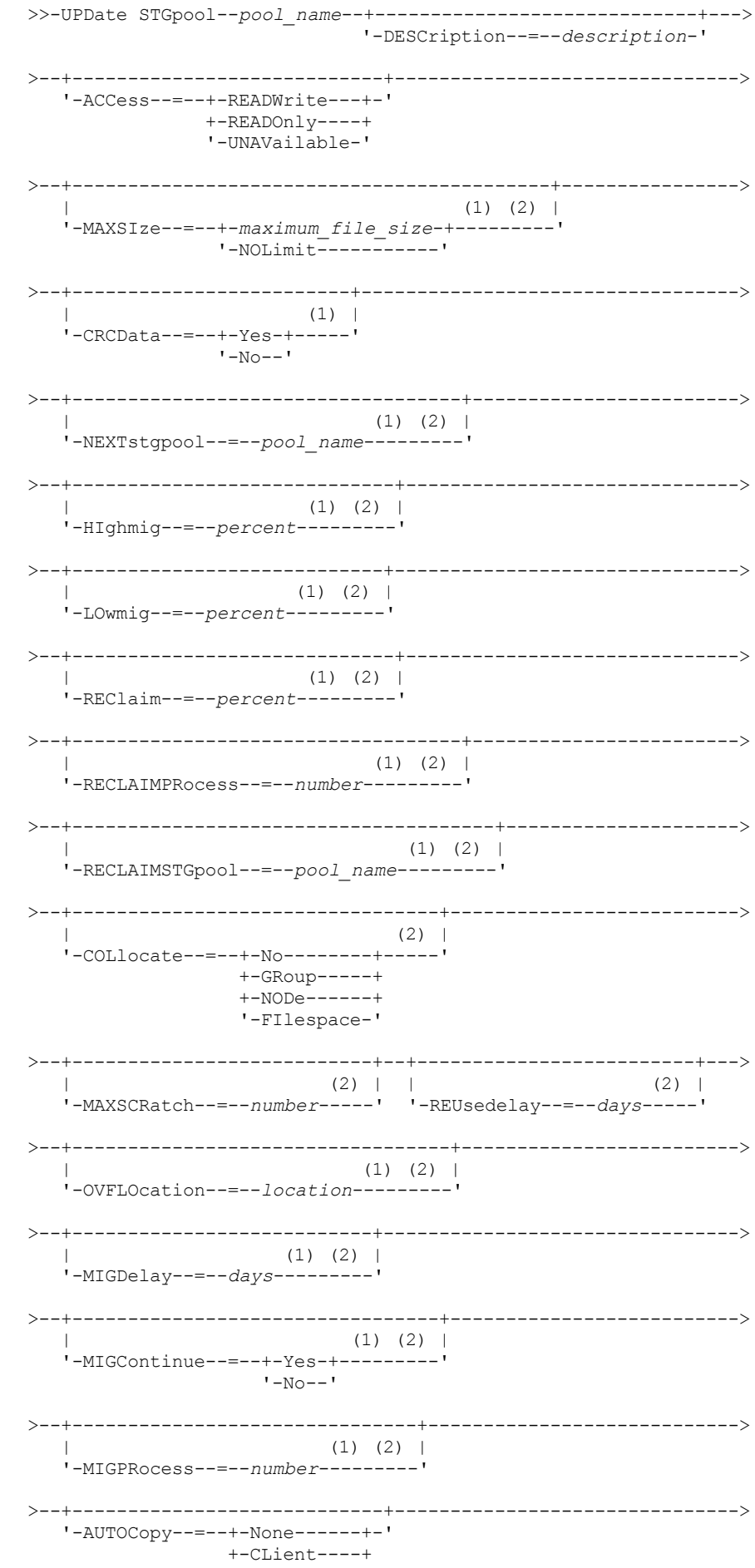
Restrictions:

1. You cannot use this command to change the data format for the storage pool.
2. If the value for DATAFORMAT is NETAPPDUMP, CELERRADUMP, or NDMPDUMP, you can modify only the following attributes:
   - DESCRIPTION
   - ACCESS
   - COLLOCATE
   - MAXSCRATCH
   - REUSEDELAY

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to be updated.

Syntax


>>-UPDate STGpool--pool_name--+----------------------------+--->
'-DESCription--=--description-'
>--+----------------------------+------------------------------>
'-ACCess--=--+-READWrite---+-'
+-READOnly----+
'-UNAVailable-'
>--+--+---------------->
| (1) (2) |
'-MAXSIze--=--+-maximum_file_size-+---------'
'-NOLimit-----------'
>--+------------------------+-------------------------------->
| (1) |
'-CRCData--=--+-Yes-+-----'
'-No--'
>--+--------------------------------+------------------------>
| (1) (2) |
'-NEXTstgpool--=--pool_name---------'
>--+----------------------------+---------------------------->
| (1) (2) |
'-HIghmig--=--percent---------'
>--+----------------------------+---------------------------->
| (1) (2) |
'-LOwmig--=--percent---------'
>--+----------------------------+---------------------------->
| (1) (2) |
'-RECLaim--=--percent---------'
>--+--------------------------------+------------------------>
| (1) (2) |
'-RECLAIMPRocess--=--number---------'
>--+-----------------------------------+--------------------->
| (1) (2) |
'-RECLAIMSTGpool--=--pool_name---------'
>--+---------------------------------+-------------------------->
| (2) |
'-COLlocate--=--+-No--------+-----'
+-GRoup-----+
+-NODe------+
'-FIlespace-'
>--+--------------------------+--+-----------------------+---->
| (2) | | (2) |
'-MAXSCRatch--=--number-----' '-REUsedelay--=--days-----'
>--+--------------------------------+------------------------>
| (1) (2) |
'-OVFLOcation--=--location---------'
>--+----------------------------+---------------------------->
| (1) (2) |
'-MIGDelay--=--days---------'
>--+--------------------------------+------------------------>
| (1) (2) |
'-MIGContinue--=--+-Yes-+---------'
'-No--'
>--+--------------------------------+------------------------>
| (1) (2) |
'-MIGPRocess--=--number---------'
>--+----------------------------+---------------------------->
'-AUTOCopy--=--+-None------+-'
+-CLient----+

Notes:

1. This parameter is not available for storage pools that use the data formats NETAPPDUMP, CELERRADUMP, or NDMPDUMP.
2. This parameter is not available for CENTERA storage pools.
3. This parameter is valid only for storage pools that are defined with a FILE-type device class.
4. This parameter is only available if the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
Specifies the name of the storage pool to be updated.

DESCription
Specifies a description of the storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
Specifies how client nodes and server processes (such as migration and reclamation) can access files in the storage pool. This parameter is optional. You can specify the following values:

READWrite
Specifies that client nodes and server processes can read and write to files stored on volumes in the storage pool.

READOnly
Specifies that client nodes can only read files from the volumes in the storage pool.

Server processes can move files within the volumes in the storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *readonly*, the storage pool is skipped when server processes attempt to write files to the storage pool.

UNAVailable
Specifies that client nodes cannot access files stored on volumes in the storage pool.

Server processes can move files within the volumes in the storage pool and can also move or copy files from this storage pool to another storage pool. However, no new writes are permitted to volumes in the storage pool from volumes outside the storage pool.

If this storage pool was specified as a subordinate storage pool (with the NEXTSTGPOOL parameter) and is defined as *unavailable*, the storage pool is skipped when server processes attempt to write files to the storage pool.

MAXSIze

Specifies the maximum size for a physical file that the server can store in the storage pool. This parameter is optional. You can specify the following values:

NOLimit

Specifies that there is no maximum size limit for physical files stored in the storage pool.

maximum_file_size

Limits the maximum physical file size. Specify an integer from 1 to 999999 terabytes, followed by a scale factor. For example, MAXSIZE=5G specifies that the maximum file size for this storage pool is 5 gigabytes. Scale factors are:

Scale factor	Meaning
K	kilobyte
M	megabyte
G	gigabyte
T	terabyte

The client estimates the size of files that are sent to the server. The client estimate is used rather than the actual amount of data that is sent to the server. Client options, such as deduplication, compression, and encryption, can cause the actual amount of data that is sent to the server to be larger or smaller than the size estimate. For example, the compression of a file might be smaller in size than the estimate, thus sending less data than the estimate. Furthermore, a binary file might be larger in size after the compression processing, thus sending more data than the estimate.

When the physical size of the storage pool exceeds the MAXSIZE parameter, the following table shows where files are typically stored.

Table 1. The location of a file according to the file size and the pool that is specified

File size	Pool specified	Result
Exceeds the maximum size	No pool is specified as the next storage pool in the hierarchy	The server does not store the file
	A pool is specified as the next storage pool in the hierarchy	The server stores the file in the next storage pool that can accept the file size

Tip: If you also specify the NEXTstgpool parameter, define one storage pool in your hierarchy to have no limit on the maximum file size by specifying the MAXSIze=NOLimit parameter. When you have at least one pool with no size limit, you ensure that no matter what its size, the server can store the file.

For multiple files that are sent in a single transaction, the server considers the size of the transaction to be the file size. If the total size of all files in the transaction is larger than the maximum size limit, the server does not store the files in the storage pool.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCData

Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

Yes

Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

No

Specifies that data is stored without CRC information.

Tip:

For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage

pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

- IBM® LTO5 and later.
- IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
- Oracle StorageTek T10000C and T10000D drives.

NEXTstgpool
: Specifies a primary storage pool to which files are migrated. You cannot migrate data from a sequential access storage pool to a random access storage pool. This parameter is optional. The next storage pool must be a primary storage pool.

  To remove an existing value, specify a null string ("").

  If this storage pool does not have a next storage pool, the server cannot migrate files from this storage pool and cannot store files that exceed the maximum size for this storage pool in another storage pool.

  When there is insufficient space available in the current storage pool, the NEXTSTGPOOL parameter for sequential access storage pools does not allow data to be stored into the next pool. In this case, the server issues a message and the transaction fails.

  For next storage pools with a device type of FILE, the server completes a preliminary check to determine whether sufficient space is available. If space is not available, the server skips to the next storage pool in the hierarchy. If space is available, the server attempts to store data in that pool. However, it is possible that the storage operation might fail because, at the time the actual storage operation is attempted, the space is no longer available.

  Restrictions:

  - To ensure that you do not create a chain of storage pools that leads to an endless loop, specify at least one storage pool in the hierarchy with no value.
  - If you specify a sequential-access pool as the next storage pool, the pool must be in either NATIVE or NONBLOCK data format.
  - Do not specify a directory-container or cloud-container storage pool.
  - Do not use this parameter to specify a storage pool for data migration.
  - This parameter is not available for storage pools that use the following data formats:
    - NETAPPDUMP
    - CELERRADUMP
    - NDMPDUMP

HIghmig
: Specifies that the server starts migration when storage pool utilization reaches this percentage. For sequential-access disk (FILE) storage pools, utilization is the ratio of data in a storage pool to the pool's total estimated data capacity, including the capacity of all scratch volumes specified for the pool. For storage pools that use tape media, utilization is the ratio of volumes that contain data to the total number of volumes in the storage pool. The total number of volumes includes the maximum number of scratch volumes. This parameter is optional. You can specify an integer 0 - 100.

  When the storage pool exceeds the high migration threshold, the server can start migration of files by volume to the next storage pool defined for the storage pool. You can set the high migration threshold to 100 to prevent migration for the storage pool.

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

LOwmig
: Specifies that the server stops migration when storage pool utilization is at or below this percentage. For sequential-access disk (FILE) storage pools, utilization is the ratio of data in a storage pool to the pool's total estimated data capacity, including the capacity of all scratch volumes specified for the pool. For storage pools that use tape media, utilization is the ratio of volumes that contain data to the total number of volumes in the storage pool. The total number of volumes includes the maximum number of scratch volumes. This parameter is optional. You can specify an integer 0 - 99.

When the storage pool reaches the low migration threshold, the server does not start migration of files from another volume. You can set the low migration threshold to 0 to allow migration to empty the storage pool.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLaim

Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the IBM Spectrum Protect™ database.

Reclamation makes the fragmented space on volumes usable again by moving any remaining unexpired files from one volume to another volume, thus making the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100.

The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

Specify a value of 50 percent or greater for this parameter so that files stored on two volumes can be combined onto a single output volume.

For storage pools that use a WORM device class, you can lower the value from the default of 100. Lowering the value allows the server to consolidate data onto fewer volumes when needed. Volumes that are emptied by reclamation can be checked out of the library, freeing slots for new volumes. Because the volumes are write-once, the volumes cannot be reused.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMPRocess

Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999. You can specify one or more reclamation processes for each primary sequential-access storage pool.
When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

- The number of sequential storage pools.
- The number of logical and physical drives that can be dedicated to the operation.

To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Assuming that the RECLAIMSTGPOOL parameter is not specified or that the reclaim storage pool has the same device class as the storage pool that is being reclaimed, each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for the two storage pools must have a mount limit of at least 16.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMSTGpool

Specifies another primary storage pool as a target for reclaimed data from this storage pool. This parameter is optional. When the server reclaims volumes for the storage pool, unexpired data is moved from the volumes that are being reclaimed to the storage pool named with this parameter.

To remove an existing value, specify a null string ("").

A reclaim storage pool is most useful for a storage pool that has only one drive in its library. When you specify this parameter, the server moves all data from reclaimed volumes to the reclaim storage pool regardless of the number of drives in the library.

To move data from the reclaim storage pool back to the original storage pool, use the storage pool hierarchy. Specify the original storage pool as the next storage pool for the reclaim storage pool.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate
Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

- A single client node
- A group of file spaces
- A group of client nodes
- A client file space

This parameter is optional.

Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required. Collocation can also impact the number of processes that are migrating disks to sequential pool.

You can specify one of the following options:

No
Specifies that collocation is disabled. During migration from disk, processes are created at a file space level.

GRoup
Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
- Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.
- During migration from disk, the server creates migration processes at the collocation group level for grouped nodes, and at the node level for ungrouped nodes.

If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
- Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces that are named A, B, C, D, and E. File spaces A and B belong to a file space collocation group but C, D, and E do not. File spaces A and B are collocated by file space collocation group, while C, D, and E are collocated by node.

- During migration from disk, the server creates migration processes at the collocation group level for grouped file spaces.

Data is collocated on the least number of sequential access volumes.

NODe
: Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

  If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

  For COLLOCATE=NODE, the server creates processes at the node level when you migrate data from disk.

FIlespace
: Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

  For COLLOCATE=FILESPACE, the server creates processes at the file space level when you migrate data from disk.

MAXSCRatch
: Specifies the maximum number of scratch volumes that the server can request. This parameter is optional. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes, you avoid having to define each volume to be used.

  The value that is specified for this parameter is used to estimate the total number of volumes available in the storage pool and the corresponding estimated capacity for the storage pool.

  Scratch volumes are automatically deleted from the storage pool when they become empty. When scratch volumes with the device type of FILE are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

  Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay
: Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. The value 0 means that a volume can be rewritten or returned to the scratch pool as soon as all files are deleted from the volume.

  By specifying this parameter, you can ensure that the database can be restored to an earlier level and database references to files in the storage pool would still be valid.

OVFLOcation
: Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the MOVE MEDIA command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.

  To remove an existing value, specify a null string ("").

  Restriction: This parameter is not available for storage pools that use the following data formats:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

MIGDelay
: Specifies the minimum number of days a file must remain in a storage pool before it becomes eligible for migration. All files on a volume must be eligible for migration before the server selects the volume for migration. To calculate a value to compare to the specified MIGDELAY, the server counts the number of days that the file has been in the storage pool.

This parameter is optional. You can specify an integer 0 - 9999.

If you want the server to count the number of days that are based only on when a file was stored and not when it was retrieved, use the NORETRIEVEDATE server option.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue
: Specifies whether you allow the server to migrate files that do not satisfy the migration delay time. This parameter is optional.

Because you can require that files remain in the storage pool for a minimum number of days, the server may migrate all eligible files to the next storage pool yet not meet the low migration threshold. This parameter allows you to specify whether the server is allowed to continue migration by migrating files that do not satisfy the migration delay time.

You can specify one of the following values:

Yes
: Specifies that, when necessary to meet the low migration threshold, the server continues to migrate files that have not been stored in the storage pool for the number of days specified by the migration delay period.

No
: Specifies that the server stops migration when no eligible files remain to be migrated, even before reaching the low migration threshold. The server does not migrate files unless the files have been stored in the storage pool for the number of days specified by the migration delay period.

Restriction: This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGPRocess
: Specifies the number of parallel processes to use for migrating the files from the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999.

When calculating the value for this parameter, consider the number of sequential storage pools that will be involved with the migration, and the number of logical and physical drives that can be dedicated to the operation. To access a sequential-access volume, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive. The number of available mount points and drives depends on other IBM Spectrum Protect and system activity and on the mount limits of the device classes for the sequential access storage pools that are involved in the migration.

For example, suppose you want to simultaneously migrate the files from volumes in two primary sequential storage pools and that you want to specify three processes for each of the storage pools. The storage pools have the same device class. Assuming that the storage pool to which files are being migrated has the same device class as the storage pool from which files are being migrated, each process requires two mount points and, if the device type is not FILE, two drives. (One drive is for the input volume, and the other drive is for the output volume.) To run six migration processes simultaneously, you need a total of at least 12 mount points and 12 drives. The device class for the storage pools must have a mount limit of at least 12.

If the number of migration processes you specify is more than the number of available mount points or drives, the processes that do not obtain mount points or drives will wait for mount points or drives to become available. If mount points or drives do not become available within the MOUNTWAIT time, the migration processes will end. For information about specifying the MOUNTWAIT time, see DEFINE DEVCLASS (Define a device class).

The IBM Spectrum Protect server will start the specified number of migration processes regardless of the number of volumes that are eligible for migration. For example, if you specify ten migration processes and only six volumes are eligible for migration, the server will start ten processes and four of them will complete without processing a volume.

Note: When you specify this parameter, consider whether the simultaneous-write function is enabled for server data migration. Each migration process requires a mount point and a drive for each copy storage pool and active-data pool that is defined to the target storage pool.

AUTOCopy

Specifies when IBM Spectrum Protect completes simultaneous-write operations. This parameter affects the following operations:

- Client store sessions
- Server import processes
- Server data-migration processes

If the AUTOCOPY option is set to `ALL` or `CLIENT`, and there is at least one storage pool that is listed in the COPYSTGPOOLS or ACTIVEDATAPOOLS options, any client-side deduplication is disabled.

If an error occurs while data is being simultaneously written to a copy storage pool or active-data pool during a migration process, the server stops writing to the failing storage pools for the remainder of the process. However, the server continues to store files into the primary storage pool and any remaining copy storage pools or active-data pools. These pools remain active for the duration of the migration process. Copy storage pools are specified using the COPYSTGPOOLS parameter. Active-data pools are specified using the ACTIVEDATAPOOLS parameter.

You can specify one of the following values:

None
: Specifies that the simultaneous-write function is disabled.

CLient
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions or server import processes. During server import processes, data is written simultaneously to only copy storage pools. Data is not written to active-data pools during server import processes.

MIGRation
: Specifies that data is written simultaneously to copy storage pools and active-data pools only during migration to this storage pool. During server data-migration processes, data is written simultaneously to copy storage pools and active-data pools only if the data does not exist in those pools. Nodes whose data is being migrated must be in a domain associated with an active-data pool. If the nodes are not in a domain associated with an active pool, the data cannot be written to the pool.

All
: Specifies that data is written simultaneously to copy storage pools and active-data pools during client store sessions, server import processes, or server data-migration processes. Specifying this value ensures that data is written simultaneously whenever this pool is a target for any of the eligible operations.

COPYSTGpools
: Specifies the names of copy storage pools where the server simultaneously writes data. You can specify a maximum of three copy pool names that are separated by commas. Spaces between the names of the copy pools are not allowed. To add or remove one or more copy storage pools, specify the pool name or names that you want to include in the updated list. For example, if the existing copy pool list includes COPY1 and COPY2 and you want to add COPY3, specify COPYSTGPOOLS=COPY1,COPY2,COPY3. To remove all existing copy storage pools that are associated with the primary storage pool, specify a null string ("") for the value (for example, COPYSTGPOOLS="").

  When you specify a value for the COPYSTGPOOLS parameter, you can also specify a value for the COPYCONTINUE parameter. For more information, see the COPYCONTINUE parameter.

  The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

  When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of copy storage pools and the COPYCONTINUE value from the primary storage pool. The primary storage pool is specified by the copy group of the management class that is bound to the data.

  The server can write data simultaneously to copy storage pools during the following operations:

  - Back up and archive operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API
  - Migration operations by IBM Spectrum Protect for Space Management clients
  - Import operations that involve copying exported file data from external media to a primary storage pool associated with a copy storage pool list

  Restrictions:

  1. This parameter is available only to primary storage pools that use NATIVE or NONBLOCK data format. This parameter is not available for storage pools that use the following data formats:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

2. Simultaneous-write operations takes precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is accepted.
3. The simultaneous-write function is not supported for NAS backup operations. If the primary storage pool specified in the DESTINATION or TOCDESTINATION in the copy group of the management class has copy storage pools defined, the copy storage pools are ignored and the data is stored into the primary storage pool only.
4. You cannot use the simultaneous-write function with CENTERA storage devices.

Attention: The function that is provided by the COPYSTGPOOLS parameter is not intended to replace the BACKUP STGPOOL command. If you use the COPYSTGPOOLS parameter, continue to use the BACKUP STGPOOL command to ensure that the copy storage pools are complete copies of the primary storage pool. There are cases when a copy might not be created. For more information, see the COPYCONTINUE parameter description.

COPYContinue

Specifies how the server reacts to a copy storage pool write failure for any of the copy storage pools that are listed in the COPYSTGPOOLS parameter. This parameter is optional. The default is YES. When you specify the COPYCONTINUE parameter, either a COPYSTGPOOLS list must exist or the COPYSTGPOOLS parameter must also be specified.

The COPYCONTINUE parameter has no effect on the simultaneous-write function during migration.

You can specify the following values:

Yes

If the COPYCONTINUE parameter is set to YES, the server will stop writing to the failing copy pools for the remainder of the session, but continue storing files into the primary pool and any remaining copy pools. The copy storage pool list is active only for the life of the client session and applies to all the primary storage pools in a particular storage pool hierarchy.

No

If the COPYCONTINUE parameter is set to NO, the server will fail the current transaction and discontinue the store operation.

Restrictions:

- The setting of the COPYCONTINUE parameter does not affect active-data pools. If a write failure occurs for any of the active-data pools, the server stops writing to the failing active-data pool for the remainder of the session, but continues storing files into the primary pool and any remaining active-data pools and copy storage pools. The active-data pool list is active only for the life of the session and applies to all the primary storage pools in a particular storage pool hierarchy.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server import. If data is being written simultaneously and a write failure occurs to the primary storage pool or any copy storage pool, the server import process fails.
- The setting of the COPYCONTINUE parameter does not affect the simultaneous-write function during server data migration. If data is being written simultaneously and a write failure occurs to any copy storage pool or active-data pool, the failing storage pool is removed and the data migration process continues. Write failures to the primary storage pool cause the migration process to fail.

ACTIVEDATApools

Specifies the names of active-data pools where the server simultaneously writes data during a client backup operation. The ACTIVEDATAPOOLS parameter is optional. Spaces between the names of the active-data pools are not allowed.

The combined total number of storage pools that are specified in the COPYSGTPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

When a data storage operation switches from a primary storage pool to a next storage pool, the next storage pool inherits the list of active-data pools from the destination storage pool specified in the copy group. The primary storage pool is specified by the copy group of the management class that is bound to the data.

The server can write data simultaneously to active-data pools only during backup operations by IBM Spectrum Protect backup-archive clients or application clients that use the IBM Spectrum Protect API.
Restrictions:

1. This parameter is available only to primary storage pools that use NATIVE or NONBLOCK data format. This parameter is not available for storage pools that use the following data formats:
   - NETAPPDUMP

- CELERRADUMP
- NDMPDUMP

2. Writing data simultaneously to active-data pools is not supported when the operation is using LAN-free data movement. Simultaneous-write operations take precedence over LAN-free data movement, causing the operations to go over the LAN. However, the simultaneous-write configuration is accepted.
3. The simultaneous-write function is not supported when a NAS backup operation is writing a TOC file. If the primary storage pool specified in the TOCDESTINATION in the copy group of the management class has active-data pools defined, the active-data pools are ignored and the data is stored into the primary storage pool only.
4. You cannot use the simultaneous-write function with CENTERA storage devices.
5. Data being imported cannot be stored in active-data pools. After an import operation, use the COPY ACTIVEDATA command to store the imported data in an active-data pool.

Attention: The function that is provided by the ACTIVEDATAPOOLS parameter is not intended to replace the COPY ACTIVEDATA command. If you use the ACTIVEDATAPOOLS parameter, use the COPY ACTIVEDATA command to ensure that the active-data pools contain all active data of the primary storage pool.

DEDUPlicate
: Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE device class.

IDENTIFYPRocess
: Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a device class associated with the FILE device type. Enter a value 1 - 50.
Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Update the primary sequential storage pool's mountable scratch volumes

Update the primary sequential storage pool that is named TAPEPOOL1 to allow as many as 10 scratch volumes to be mounted.

```
update stgpool tapepool1 maxscratch=10
```

UPDATE STGPOOL (Update a copy sequential access storage pool)

Use this command to update a copy sequential access storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to be updated.

Syntax

```
>>-UPDate STGpool--pool_name--+-----------------------------+--->
                              '-DESCription--=--description-'

>--+---------------------------+------------------------------>
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

>--+----------------------------+--+--------------------+----->
   '-COLlocate--=--+-No--------+-'  '-REClaim--=--percent-'
                   +-GRoup-----+
                   +-NODe------+
                   '-FIlespace-'

>--+--------------------------+------------------------------->
   '-RECLAIMPRocess--=--number-'

>--+------------------------------------+--------------------->
```

```
   '-OFFSITERECLAIMLimit--=--+-NOLimit-+-'
                             '-number--'

>--+----------------------+--+--------------------+----------->
   '-MAXSCRatch--=--number-'  '-REUsedelay--=--days-'

>--+--------------------------+--+---------------------+-------->
   '-OVFLOcation--=--location-'  '-CRCData--=--+-Yes-+-'
                                               '-No--'

>--+-----------------------------+----------------------------->
   '-DEDUPlicate--=--+-No------+-'
                     |     (1) |
                     '-Yes-----'

>--+-------------------------------+-------------------------><
   |                           (2) |
   '-IDENTIFYPRocess--=--number-----'
```

Notes:

1. This parameter is valid only for storage pools that are defined with a FILE-type device class.
2. This parameter is only available if the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
: Specifies the name of the copy storage pool to be updated.

DESCription
: Specifies a description of the copy storage pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
: Specifies how client nodes and server processes (such as reclamation) can access files in the copy storage pool. This parameter is optional. You can specify the following values:

  READWrite
  : Specifies that files can be read from and written to the volumes in the copy storage pool.

  READOnly
  : Specifies that client nodes can read only files that are stored on the volumes in the copy storage pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the copy storage pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the copy storage pool from volumes outside the storage pool. A storage pool cannot be backed up to the copy storage pool.

  UNAVailable
  : Specifies that client nodes cannot access files that are stored on volumes in the copy storage pool.

    Server processes can move files within the volumes in the storage pool. The server can use files in the copy storage pool to restore files to primary storage pools. However, no new writes are allowed to volumes in the copy storage pool from volumes outside the storage pool. A storage pool cannot be backed up to the copy storage pool.

COLlocate
: Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

  - A single client node
  - A group of file spaces
  - A group of client nodes
  - A client file space

  This parameter is optional.

  Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required.

You can specify one of the following options:

No
: Specifies that collocation is disabled.

GRoup
: Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

  If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

  For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

  - Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
  - Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.

  If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

  - Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
  - Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces named A, B, C, D, and E. File spaces A and B belong to a filespace collocation group but C, D, and E do not. File spaces A and B are collocated by filespace collocation group, while C, D, and E are collocated by node.

  Data is collocated on the least amount of sequential access volumes.

NODe
: Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

  If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

FIlespace
: Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

RECLaim
: Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the IBM Spectrum Protect™ database.

  Reclamation makes the fragmented space on volumes usable again by moving any remaining active files from one volume to another volume, thus making the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100. The value 100 means that reclamation is not completed.

  The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

  If you change the value from the default of 100, specify a value of 50 percent or greater so that files stored on two volumes can be combined onto a single output volume.

When a copy pool volume that is offsite becomes eligible for reclamation, the reclamation process attempts to obtain the active files on the reclaimable volume from a primary or copy storage pool that is onsite. The process then writes these files to an available volume in the original copy storage pool. Effectively, these files are moved back to the onsite location. However, the files can be obtained from the offsite volume after a disaster if a database backup is used that references the files on the offsite volume. Because of the way reclamation works with offsite volumes, use it carefully with copy storage pools.

RECLAIMPRocess
Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999.
When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

- The number of sequential storage pools.
- The number of logical and physical drives that can be dedicated to the operation.

To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for each storage pool must have a mount limit of at least eight.

You can specify one or more reclamation processes for each copy storage pool. You can specify multiple concurrent reclamation processes for a single copy storage pool, which makes better use of your available tape drives or FILE volumes. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

OFFSITERECLAIMLimit
Specifies the number of offsite volumes that space is reclaimed from during reclamation for this storage pool. This parameter is optional. You can specify the following values:

NOLimit
Specifies that you want to reclaim the space in all of your offsite volumes.

number
Specifies the number of offsite volumes to reclaim space from. You can specify an integer 0 - 99999. A value of zero means that none of the offsite volumes are reclaimed.
Tip:

To determine the value for the OFFSITERECLAIMLIMIT, use the statistical information in the message that is issued at the end of the offsite volume reclamation operation. The statistical information includes the following items:

- The number of offsite volumes that were processed
- The number of parallel processes that were used
- The total amount of time required for the processing

The order in which offsite volumes are reclaimed is based on the amount of unused space in a volume. (Unused space includes both space that has never been used on the volume and space that has become empty because of file deletion.) Volumes with the largest amount of unused space are reclaimed first.

For example, suppose a copy storage pool contains three volumes: VOL1, VOL2, and VOL3. VOL1 has the largest amount of unused space, and VOL3 has the least amount of unused space. Suppose further that the percentage of unused space in each of the three volumes is greater than the value of the RECLAIM parameter. If you do not specify a value for the OFFSITERECLAIMLIMIT parameter, all three volumes will be reclaimed when the reclamation runs. If you specify a value of 2, only VOL1 and VOL2 will be reclaimed when the reclamation runs. If you specify a value of 1, only VOL1 will be reclaimed.

MAXSCRatch
Specifies the maximum number of scratch volumes that the server can request for this storage pool. This parameter is optional. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes as needed, you avoid having to define each volume to be used.

The value that is specified for this parameter is used to estimate the total number of volumes available in the copy storage pool and the corresponding estimated capacity for the copy storage pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. However, if the access mode for a scratch volume is OFFSITE, the volume is not deleted from the copy storage pool until the access mode is changed. An administrator can query the server for empty, offsite scratch volumes and return them to the onsite location.

When scratch volumes with the device type of FILE become empty and are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The IBM Spectrum Protect server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay

Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. A value of 0 means that a volume can be rewritten or returned to the scratch pool as soon as all files are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to files in the copy storage pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. The number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

OVFLOcation

Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the MOVE MEDIA command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.

To remove an existing value, specify a null string ("").

CRCData

Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

Yes

Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

No

Specifies that data is stored without CRC information.

Tip:

For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

- IBM® LTO5 and later.
- IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
- Oracle StorageTek T10000C and T10000D drives.

DEDUPlicate

Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE-type device class.

IDENTIFYPRocess

Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. Enter a value 1 - 50.
Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes

and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Update a copy storage pool to a 30-day volume reuse and to collocate files by client node

Update the copy storage pool that is named TAPEPOOL2 to change the delay for volume reuse to 30 days and to collocate files by client node.

```
update stgpool tapepool2 reusedelay=30 collocate=node
```

Related reference:
SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)

UPDATE STGPOOL (Update an active-data sequential access)

Use this command to update an active-data pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege for the storage pool to be updated.

Syntax

Notes:

1. This parameter is valid only for storage pools that are defined with a FILE-type device class.
2. This parameter is only available if the value of the DEDUPLICATE parameter is YES.

Parameters

pool_name (Required)
Specifies the name of the active-data pool to be updated.

DESCription
Specifies a description of the active-data pool. This parameter is optional. The maximum length of the description is 255 characters. Enclose the description in quotation marks if it contains any blank characters. To remove an existing description, specify a null string ("").

ACCess
Specifies how client nodes and server processes (such as reclamation) can access files in the active-data pool. This parameter is optional. You can specify the following values:

READWrite
Specifies that files can be read from and written to the volumes in the active-data pool.

READOnly
Specifies that client nodes can read only files that are stored on the volumes in the active-data pool.

Server processes can move files within the volumes in the storage pool. The server can use files in the active-data pool to restore active versions of backup files to primary storage pools. However, no new writes are allowed to volumes in the active-data pool from volumes outside the storage pool. A storage pool cannot be copied to the active-data pool.

UNAVailable
Specifies that client nodes cannot access files that are stored on volumes in the active-data pool.

Server processes can move files within the volumes in the storage pool. The server can use files in the active-data pool to restore active versions of backup files to primary storage pools. However, no new writes are allowed to volumes in the active-data pool from volumes outside the storage pool. A storage pool cannot be copied to the active-data pool.

COLlocate
Specifies whether the server attempts to keep data, which is stored on as few volumes as possible, that belong to one of the following candidates:

- A single client node
- A group of file spaces
- A group of client nodes
- A client file space

This parameter is optional.

Collocation reduces the number of sequential access media mounts for restore, retrieve, and recall operations. However, collocation increases both the amount of server time that is needed to collocate files for storing and the number of volumes required.

You can specify one of the following options:

No
Specifies that collocation is disabled.

GRoup
Specifies that collocation is enabled at the group level for client nodes or file spaces. For collocation groups, the server attempts to put data for nodes or file spaces that belong to the same collocation group on as few volumes as possible.

If you specify COLLOCATE=GROUP but do not define any collocation groups, or if you do not add nodes or file spaces to a collocation group, data is collocated by node. Consider tape usage when you organize client nodes or file spaces into collocation groups.

For example, if a tape-based storage pool consists of data from nodes and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates the data by group for grouped nodes. Whenever possible, the server collocates data that belongs to a group of nodes on a single tape or on as few tapes as possible. Data for a single node can also be spread across several tapes that are associated with a group.
- Collocates the data by node for ungrouped nodes. Whenever possible, the server stores the data for a single node on a single tape. All available tapes that already have data for the node are used before available space on any other tape is used.

If a tape-based storage pool consists of data from grouped file spaces and you specify COLLOCATE=GROUP, the server completes the following actions:

- Collocates by group, the data for grouped file spaces only. Whenever possible, the server collocates data that belongs to a group of file spaces on a single tape or on as few tapes as possible. Data for a single file space can also be spread across several tapes that are associated with a group.
- Collocates the data by node (for file spaces that are not explicitly defined to a file space collocation group). For example, node1 has file spaces named A, B, C, D, and E. File spaces A and B belong to a filespace collocation group but C, D, and E do not. File spaces A and B are collocated by filespace collocation group, while C, D, and E are collocated by node.

Data is collocated on the least amount of sequential access volumes.

NODe
: Specifies that collocation is enabled at the client node level. For collocation groups, the server attempts to put data for one node on as few volumes as possible. If the node has multiple file spaces, the server does not try to collocate those file spaces. For compatibility with an earlier version, COLLOCATE=YES is still accepted by the server to specify collocation at the client node level.

  If a storage pool contains data for a node that is a member of a collocation group and you specify COLLOCATE=NODE, the data is collocated by node.

FIlespace
: Specifies that collocation is enabled at the file space level for client nodes. The server attempts to place data for one node and file space on as few volumes as possible. If a node has multiple file spaces, the server attempts to place data for different file spaces on different volumes.

RECla im
: Specifies when the server reclaims a volume, which is based on the percentage of reclaimable space on a volume. Reclaimable space is the amount of space that is occupied by files that are expired or deleted from the IBM Spectrum Protect™ database.

  Reclamation makes the fragmented space and space occupied by inactive backup files on volumes usable again by moving any remaining unexpired files and active backup files from one volume to another volume. This action makes the original volume available for reuse. This parameter is optional. You can specify an integer 1 - 100. The value 100 means that reclamation is not completed.

  The server determines that the volume is a candidate for reclamation if the percentage of reclaimable space on a volume is greater than the reclamation threshold of the storage pool.

  If you change the value from the default of 60, specify a value of 50 percent or greater so that files stored on two volumes can be combined onto a single output volume.

  When an active-data pool volume that is offsite becomes eligible for reclamation, the reclamation process attempts to obtain the active files on the reclaimable volume from a primary or active-data pool that is onsite. The process then writes these files to an available volume in the original active-data pool. Effectively, these files are moved back to the onsite location. However, the files can be obtained from the offsite volume after a disaster if a database backup is used that references the files on the offsite volume. Because of the way reclamation works with offsite volumes, use it carefully with active-data pools.

RECLAIMPRocess
: Specifies the number of parallel processes to use for reclaiming the volumes in this storage pool. This parameter is optional. Enter a value 1 - 999.
  When you calculate the value for this parameter, consider the following resources that are required for reclamation processing:

  - The number of sequential storage pools.
  - The number of logical and physical drives that can be dedicated to the operation.

To access sequential volumes, IBM Spectrum Protect uses a mount point and, if the device type is not FILE, a physical drive.

For example, suppose that you want to reclaim the volumes from two sequential storage pools simultaneously and that you want to specify four processes for each of the storage pools. The storage pools have the same device class. Each process requires two mount points and, if the device type is not FILE, two drives. (One of the drives is for the input volume, and the other drive is for the output volume.) To run eight reclamation processes simultaneously, you need a total of at least 16 mount points and 16 drives. The device class for each storage pool must have a mount limit of at least eight.

You can specify one or more reclamation processes for each active-data pool. You can specify multiple concurrent reclamation processes for a single active-data pool, which makes better use of your available tape drives or FILE volumes. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

OFFSITERECLAIMLimit
Specifies the number of offsite volumes that space is reclaimed from during reclamation for this storage pool. This parameter is optional. You can specify the following values:

NOLimit
Specifies that you want to reclaim the space in all of your offsite volumes.

number
Specifies the number of offsite volumes to reclaim space from. You can specify an integer 0 - 99999. A value of zero means that none of the offsite volumes are reclaimed.
Tip:

To determine the value for the OFFSITERECLAIMLIMIT, use the statistical information in the message that is issued at the end of the offsite volume reclamation operation. The statistical information includes the following items:

- The number of offsite volumes that were processed
- The number of parallel processes that were used
- The total amount of time required for the processing

The order in which offsite volumes are reclaimed is based on the amount of unused space in a volume. (Unused space includes both space that has never been used on the volume and space that has become empty because of file deletion.) Volumes with the largest amount of unused space are reclaimed first.

For example, suppose an active-data pool contains three volumes: VOL1, VOL2, and VOL3. VOL1 has the largest amount of unused space, and VOL3 has the least amount of unused space. Suppose further that the percentage of unused space in each of the three volumes is greater than the value of the RECLAIM parameter. If you do not specify a value for the OFFSITERECLAIMLIMIT parameter, all three volumes are reclaimed when the reclamation runs. If you specify a value of 2, only VOL1 and VOL2 are reclaimed when the reclamation runs. If you specify a value of 1, only VOL1 is reclaimed.

MAXSCRatch
Specifies the maximum number of scratch volumes that the server can request for this storage pool. This parameter is optional. You can specify an integer 0 - 100000000. By allowing the server to request scratch volumes as needed, you avoid having to define each volume to be used.

The value that is specified for this parameter is used to estimate the total number of volumes available in the active-data pool and the corresponding estimated capacity for the active-data pool.

Scratch volumes are automatically deleted from the storage pool when they become empty. However, if the access mode for a scratch volume is OFFSITE, the volume is not deleted from the active-data pool until the access mode is changed. An administrator can query the server for empty, offsite scratch volumes and return them to the onsite location.

When scratch volumes with the device type of FILE become empty and are deleted, the space that the volumes occupied is freed by the server and returned to the file system.

Tip: For server-to-server operations that use virtual volumes and that store a small amount of data, consider specifying a value for the MAXSCRATCH parameter that is higher than the value you typically specify for write operations to other types of volumes. After a write operation to a virtual volume, IBM Spectrum Protect marks the volume as FULL, even if the value of the MAXCAPACITY parameter on the device-class definition is not reached. The IBM Spectrum Protect server does not keep virtual volumes in FILLING status and does not append to them. If the value of the MAXSCRATCH parameter is too low, server-to-server operations can fail.

REUsedelay
Specifies the number of days that must elapse after all files are deleted from a volume before the volume can be rewritten or returned to the scratch pool. This parameter is optional. You can specify an integer 0 - 9999. A value of 0 means that a

volume can be rewritten or returned to the scratch pool as soon as all files are deleted from the volume.
Tip: Use this parameter to ensure that when you restore the database to an earlier level, database references to files in the active-data pool are still valid. You must set this parameter to a value greater than the number of days you plan to retain the oldest database backup. The number of days that are specified for this parameter must be the same as the number specified for the SET DRMDBBACKUPEXPIREDAYS command.

OVFLOcation
Specifies the overflow location for the storage pool. The server assigns this location name to a volume that is ejected from the library by the MOVE MEDIA command. This parameter is optional. The location name can be a maximum length of 255 characters. Enclose the location name in quotation marks if the location name contains any blank characters.

To remove an existing value, specify a null string ("").

CRCData
Specifies whether a cyclic redundancy check (CRC) validates storage pool data when audit volume processing occurs on the server. This parameter is only valid for NATIVE data format storage pools. This parameter is optional. The default value is NO. By setting CRCDATA to YES and scheduling an AUDIT VOLUME command, you can continually ensure the integrity of data that is stored in your storage hierarchy. You can specify the following values:

Yes
Specifies that data is stored containing CRC information, allowing for audit volume processing to validate storage pool data. This mode impacts performance because more processing is required to calculate and compare CRC values between the storage pool and the server.

No
Specifies that data is stored without CRC information.

Tip:

For storage pools that are associated with the 3592, LTO, or ECARTRIDGE device type, logical block protection provides better protection against data corruption than CRC validation for a storage pool. If you specify CRC validation for a storage pool, data is validated only during volume auditing operations. Errors are identified after data is written to tape.

To enable logical block protection, specify a value of READWRITE for the LBPROTECT parameter on the DEFINE DEVCLASS and UPDATE DEVCLASS commands for the 3592, LTO, or ECARTRIDGE device types. Logical block protection is supported only on the following types of drives and media:

- IBM® LTO5 and later.
- IBM 3592 Generation 3 drives and later with 3592 Generation 2 media and later.
- Oracle StorageTek T10000C and T10000D drives.

DEDUPlicate
Specifies whether the data that is stored in this storage pool is deduplicated. This parameter is optional and is valid only for storage pools that are defined with a FILE-type device class.

IDENTIFYPRocess
Specifies the number of parallel processes to use for server-side data deduplication. This parameter is optional and is valid only for storage pools that are defined with a FILE device class. Enter a value 1 - 50.
Remember: Data deduplication processes can be either active or idle. Processes that are working on files are active. Processes that are waiting for files to work on are idle. Processes remain idle until volumes with data to be deduplicated become available. The output of the QUERY PROCESS command for data deduplication includes the total number of bytes and files that have been processed since the process first started. For example, if a data deduplication process processes four files, becomes idle, and then processes five more files, then the total number of files processed is nine. Processes end only when canceled or when the number of data-deduplication processes for the storage pool is changed to a value less than the number currently specified.

Example: Update an active data pool

Update the active-data pool that is named TAPEPOOL2 to change the delay for volume reuse to 30 days and to collocate files by client node.

```
update stgpool tapepool3 reusedelay=30 collocate=node
```

Related reference:
SET DRMDBBACKUPEXPIREDAYS (Specify DB backup series expiration)
AIX | Linux | Windows

UPDATE STGPOOLDIRECTORY (Update a storage pool directory)

Use this command to update a storage pool directory.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax

```
>>-UPDate STGPOOLDIRectory--pool_name--directory---------------->

                                  .-MAXPRocess--=--4------.
>----ACCess--=--+-READWrite---+----+----------------------+---->
                +-READOnly----+    '-MAXProcess--=--number-'
                +-DEStroyed---+
                '-UNAVailable-'

   .-Wait--=--No------.
>--+------------------+-----------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameters

pool_name (Required)
: Specifies the storage pool that contains the directory to update. This parameter is required.

directory (Required)
: Specifies a file system directory of the storage pool. This parameter is required.

ACCess (Required)
: Specifies how client nodes and server processes can access files in the storage pool directory. This parameter is required. The following values are possible:

  READWrite
  : Specifies that files can be read from and written to the storage pool directory.

  READOnly
  : Specifies that files can be read from the storage pool directory.

  DEStroyed
  : Specifies that files are permanently damaged and must be destroyed in the storage pool directory. Use this access mode to indicate that an entire storage pool directory must be recovered.
    Tips:

    - Mark storage pool directories as `DESTROYED` before you complete data recovery. When the storage pool directory is marked as destroyed, you can recover data extents on the target replication server.
    - Use the MAXPROCESS parameter to specify the number of parallel processes that you can use to update a storage pool directory.

  UNAVailable
  : Specifies that files cannot be accessed on the storage pool directory in the storage pool.

MAXPRocess
: Specifies the maximum number of parallel processes to use for updating a storage pool directory. This parameter is optional. You can enter a value in the range 1 - 99. The default value is 4.
  Restriction: You can use this parameter only when you specify the ACCESS=DESTROYED parameter.

  When you specify the ACCESS=DESTROYED parameter, each container in the storage pool directory is updated by one process. If the maximum number of parallel processes is larger than or equal to the number of containers that must be updated, only one process is created for each container. If the number of containers exceeds the value of the MAXPROCESS parameter, the command waits for the child processes to finish before any new processes can begin.

Wait

This optional parameter specifies whether to wait for the IBM Spectrum Protect™ server to complete processing this command in the foreground. The default is NO. You can specify the following values:

No
: The server processes this command in the background and you can continue with other tasks while the command is processing. Messages that are related to the background process are shown either in the activity log file or the server console, depending on where the messages are logged.

Yes
: The server processes this command in the foreground. The operation must complete processing before you can continue with other tasks. Messages are shown either in the activity log file or the server console, or both, depending on where the messages are logged.
Restriction: You cannot specify WAIT=YES from the server console.

Example: Update a storage pool directory to destroy it

Update a storage pool directory that is named DIR1 in storage pool POOL1 to mark it as destroyed.

```
update stgpooldirectory pool1 dir1 access=destroyed
```

Example: Update a storage pool directory to destroy it in a cloud-container storage pool

Update a storage pool directory that is named DIR3 in cloud-container storage pool CLOUDLOCALDISK1 to mark it as destroyed.

```
update stgpooldirectory cloudlocaldisk1 dir3 access=destroyed
```

Example: Update a storage pool directory to make it unavailable

When the storage pool directory is unavailable, the server does not read or write data to the directory. To update the access mode to unavailable for a storage pool directory, `dir1`, in a storage pool that is named `pool1`, issue the following command:

```
update stgpooldirectory pool1 dir1 access=unavailable
```

Table 1. Commands related to UPDATE STGPOOLDIRECTORY

Command	Description
DEFINE STGPOOL	Defines a storage pool as a named collection of server storage media.
DEFINE STGPOOLDIRECTORY	Defines a storage pool directory to a directory-container or cloud-container storage pool.
DELETE STGPOOLDIRECTORY	Deletes a storage pool directory from a directory-container or cloud-container storage pool.
QUERY STGPOOLDIRECTORY	Displays information about storage pool directories.

UPDATE STGRULE (Update a storage rule)

Use this command to update a storage rule.

The UPDATE STGRULE command takes several forms. The syntax and parameters for each form are defined separately.

Table 1. Commands related to UPDATE STGRULE

Command	Description
DEFINE STGRULE (auditing)	Defines a storage rule for auditing storage pools.
DEFINE STGRULE (data deduplication statistics)	Defines a storage rule for generating data deduplication statistics.
DEFINE STGRULE (reclaiming)	Defines a storage rule for reclaiming cloud-container storage pools.
DEFINE STGRULE (tiering)	Defines a storage rule for tiering.
DELETE STGRULE	Deletes storage rules.

Command	Description
QUERY STGRULE	Displays storage rule information.

- UPDATE STGRULE (Update a rule for auditing a storage pool)
  Use this command to update a rule that schedules audit operations for a storage pool.
- UPDATE STGRULE (Update a storage rule for generating data deduplication statistics)
  Use this command to update a storage rule for generating data deduplication statistics.
- UPDATE STGRULE (Update a storage rule for reclaiming cloud containers)
  Use this command to update a storage rule for reclaiming space in cloud-container storage pools.
- UPDATE STGRULE (Update a storage rule for tiering)
  Use this command to update a storage rule for one or more storage pools. The storage rule schedules tiering between container storage pools. You can update one or more storage rules for a container storage pool.

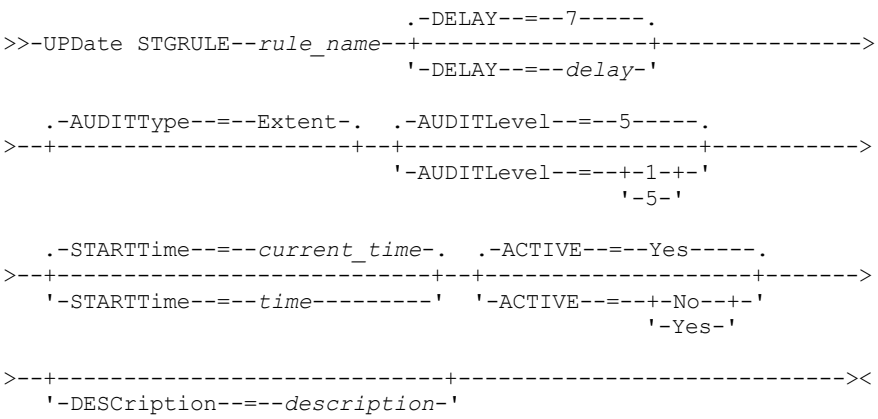
UPDATE STGRULE (Update a rule for auditing a storage pool)

Use this command to update a rule that schedules audit operations for a storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax



Parameters

rule_name (Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

DELAY
: Specifies the interval, in days, between audit operations. This parameter is optional. The default value is 7 days. You can specify an integer in the range 1 - 9999.

AUDITType
: Specifies the audit type. This parameter is optional. You can specify the following value:

  Extent
  : Specifies that only extents are audited. This is the default value.
    Restriction: In IBM Spectrum Protect™ Version 8.1.5, you can use the audit storage rule only to audit extents. Objects are not audited.

AUDITLevel
: Specifies the level of the audit. This parameter is optional. The following values are possible:

  1
  : Specifies a minimal audit operation of the extents in the storage pool.

  5
  : Specifies a full audit operation of the extents in the storage pool. This is the default value.

STARTTime
Specifies the time for the beginning of the window in which the storage rule is first processed. The default is the current time. This parameter is optional.
You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
Specifies whether storage rule processing occurs. This parameter is optional. The following values are possible:

Yes
Specifies that the storage rule is active. The storage rule is processed at the scheduled time. This is the default value.
No
Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

DESCription
Specifies a description of the storage rule. This parameter is optional. The maximum length of the description is 255 characters. If the description includes spaces, enclose the description in quotation marks.

Update a rule for an extent-level audit operation

Update a storage rule, AUDITACCOUNTING, to schedule a full, extent-level audit of data starting at 3 AM. The audit operation takes place every 14 days:

```
update stgrule auditaccounting delay=14 auditlevel=5 starttime=03:00:00
```

Related commands

Table 1. Commands related to UPDATE STGRULE

Command	Description
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.
UPDATE STGRULE (auditing)	Updates a storage rule for auditing storage pools.

UPDATE STGRULE (Update a storage rule for generating data deduplication statistics)

Use this command to update a storage rule for generating data deduplication statistics.

Privilege class

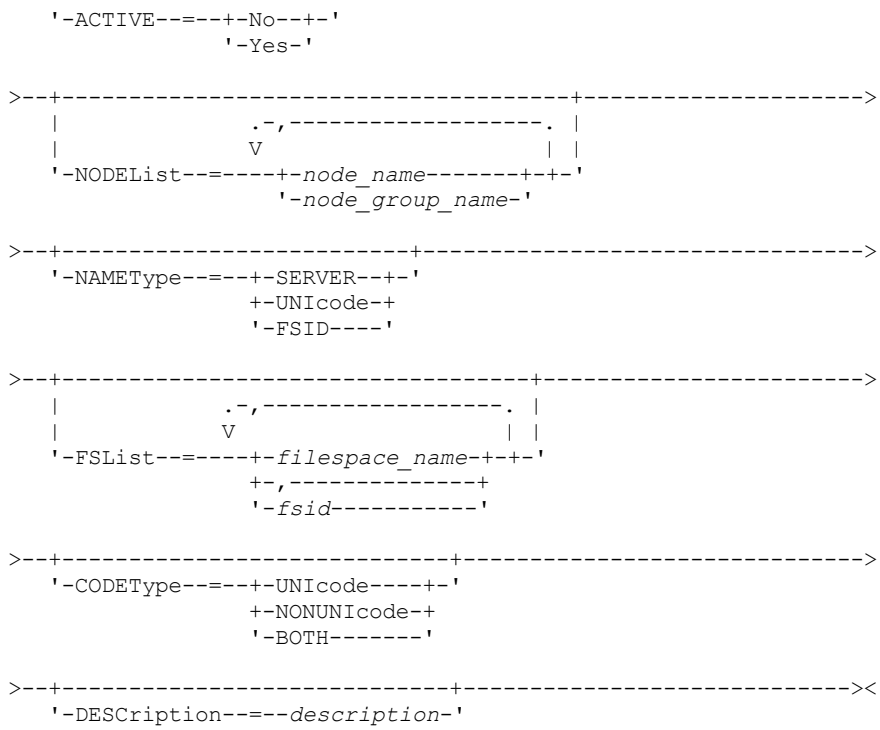
To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax

```
>>-UPDate STGRULE--rule_name--+-----------------+--------------->
                              '-DELAY--=--delay-'

>--+----------------------+--+--------------------+------------>
   '-MAXPRocess--=--number-'  '-STARTTime--=--time-'

>--+--------------------+---------------------------------------->
```



Parameters

rule_name (Required)
: Specifies the name of the storage rule. The name must be unique, and the maximum length is 30 characters.

DELAY
: Specifies the number of days to wait before the statistics are generated. You can specify an integer in the range 0 - 9999.

MAXProcess
: Specifies the maximum number of parallel processes to collect statistics for each storage pool that is specified. This parameter is optional. You can enter a value in the range 1 - 99. For example, if you have 4 storage pools and you specify a value of 8, 32 processes are started.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.
You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
: Specifies whether storage rule processing occurs. This parameter is optional. The following values are possible:

  No
  : Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

  Yes
  : Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

NODEList
: Specifies the name of the client node or defined group of client nodes for which data deduplication statistics are collected. You can also specify a combination of client node names and client-node group names. To specify multiple client node names or client-node group names, separate the names with commas with no intervening spaces. You can use wildcard

characters with client node names but not with client-node group names. The specified value can have a maximum of 1024 characters. If you enter an asterisk (*), information is shown for all client nodes. This parameter is optional.

NAMEType
Specifies how you want the server to interpret the file space names that you enter. Use this parameter when IBM Spectrum Protect™ clients have file spaces that are in Unicode format, and are on Windows, NetWare, or Macintosh OS X operating systems. This parameter is optional.
This parameter is required if you specify a node name and a file space name or FSID.
Restriction: When you specify this parameter, the file space name cannot contain an asterisk.

You can specify one of the following values:

SERVER
The server uses the server's code page to interpret the file space names.
UNIcode
The server converts the file space name that is entered from the server code page to the UTF-8 code page. The success of the conversion depends on the characters in the name and the server's code page.
Tip: Conversion can fail if the string includes characters that are not available in the server code page, or if the server cannot access system conversion routines.
FSID
The server interprets the file space names as their FSIDs.

FSList
Specifies the names of one or more file spaces for which data deduplication statistics are collected. This parameter is optional. You can use wildcard characters to specify this name. The specified value can have a maximum of 1024 characters. You can specify one of the following values:

*
Specify an asterisk (*) to show information for all file spaces or IDs.
filespace_name
Specifies the name of the file space. You can specify more than one file space by separating the names with commas and no intervening spaces.
FSID
Specifies the name of a file space identifier. This parameter is valid for clients with file spaces that are in Unicode format. Specify more than one file space by separating the names with commas and no intervening spaces.

For clients with file spaces that are in Unicode format, you can enter either a file space name or an FSID. If you enter a file space name, the server might have to convert the file space name that you enter. For example, the server might have to convert the name that you enter from the server's code page to Unicode.
Restrictions: The following restrictions apply to file space names and FSIDs:

- You must specify a node name if you specify a file space name.
- Do not specify both file space names and FSIDs on the same command.

CODEType
Specifies what type of file spaces to include in the record. Use this parameter only when you enter an asterisk to display information about all file spaces. This parameter is optional. Specify one of the following values:

UNIcode
Include file spaces that are in Unicode format.
NONUNIcode
Include file spaces that are not in Unicode format.
BOTH
Include file spaces regardless of code page type.

DESCription
Specifies a description of the storage rule. This parameter is optional.

Update a rule to generate data deduplication statistics

Update a storage rule that is named MYSTAT1 to generate data deduplication statistics. Limit the scope to the node that is named NODE1:

```
update stgrule mystat1 nodelist=node1
```

Related commands

Table 1. Commands related to UPDATE STGRULE

Command	Description
DEFINE STGRULE (data deduplication statistics)	Defines a storage rule for generating data deduplication statistics.
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.

UPDATE STGRULE (Update a storage rule for reclaiming cloud containers)

Use this command to update a storage rule for reclaiming space in cloud-container storage pools.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.
Restriction: You can configure a cloud reclamation rule for a storage pool only on a Microsoft Azure cloud computing system or on a cloud computing system with the Simple Storage Service (S3) protocol.

Syntax

```
>>-UPDate STGRULE--rule_name--+-------------------------+------>
                              '-PCTUnused--=--percentage-'

>--+----------------------+--+---------------------+---------->
   '-MAXPRocess--=--number-'  '-DUration--=--minutes-'

>--+--------------------+--+--------------------+--------------->
   '-STARTTime--=--time-'  '-ACTIVE--=--+-No--+-'
                                        '-Yes-'

>--+----------------------------+----------------------------><
   '-DESCription--=--description-'
```

Parameters

rule_name (Required)
: Specifies the name of the storage rule.

PCTUnused
: Specifies the percentage of the cloud container that is no longer in use. This parameter is optional. After unused space reaches the specified value, the cloud container is reclaimed. You can specify an integer in the range 50 - 99.

MAXProcess
: Specifies the maximum number of parallel processes for each reclamation operation. This parameter is optional. You can specify an integer in the range 1 - 99.

DUration
: Specifies the maximum number of minutes that the storage rule runs before it is automatically canceled. You can specify a number in the range 60 - 1440. If you do not specify a value, the duration is not updated. You can specify the NOLIMIT parameter to allow the rule to run to completion. This parameter is optional.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.
You can specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00

Value	Description	Example
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
Specifies whether the storage rule processing occurs. This parameter is optional. The following values are possible:

No
Specifies that the storage rule is inactive. The storage rule is not processed at the scheduled time.

Yes
Specifies that the storage rule is active. The storage rule is processed at the scheduled time.

DESCription
Specifies a description of the storage rule. This parameter is optional.

Update a rule to reclaim cloud containers

Update a storage rule that is named RECLAIMRULE to reclaim cloud containers that no longer use 60 percent of their space. Specify a start time of 23:30:00:

```
update stgrule reclaimrule pctunused=60 starttime=23:30:00
```

Related commands

Table 1. Commands related to UPDATE STGRULE

Command	Description
DEFINE STGRULE (reclaiming)	Defines a storage rule for reclaiming cloud-container storage pools.
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.

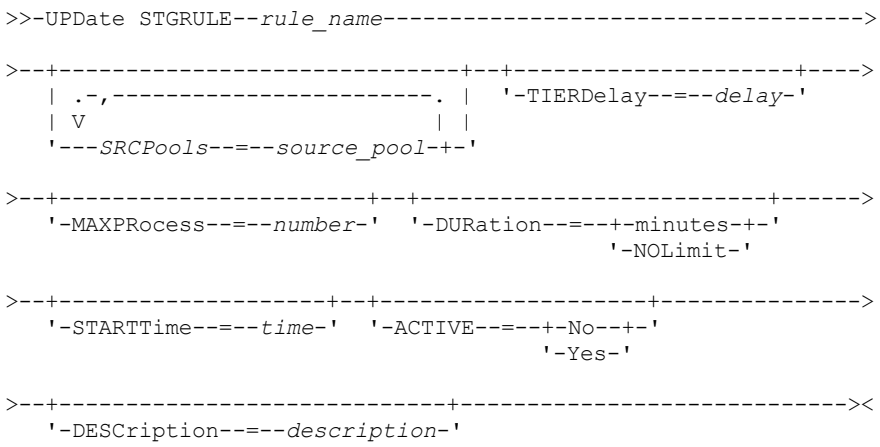
UPDATE STGRULE (Update a storage rule for tiering)

Use this command to update a storage rule for one or more storage pools. The storage rule schedules tiering between container storage pools. You can update one or more storage rules for a container storage pool.

Privilege class

To issue this command, you must have system privilege, unrestricted storage privilege, or restricted storage privilege.

Syntax



Parameters

rule_name(Required)
: Specifies the name of the storage rule. The maximum length of the name is 30 characters.

SRCPools
: Specifies the name of one or more directory-container storage pools from which objects are tiered to the target storage pool. To specify multiple storage pools, separate the names with commas with no intervening spaces.

TIERDelay
: Specifies the number of days to wait before the storage rule tiers objects to the next storage pool. You can specify an integer in the range 0 - 9999. The parameter value applies to all files in the storage pool.

MAXProcess
: Specifies the maximum number of parallel processes to complete the storage rule for each source storage pool that is specified. This parameter is optional. Enter a value in the range 1 - 99. For example, if you have 4 source storage pools and you specify the default value of 8 for this parameter, 32 processes are started.

DUration
: Specifies the maximum number of minutes that the storage rule runs before it is automatically canceled. You can specify a number in the range 60 - 1440. If you specify a value of NOLimit, the storage rule runs until it is completed. This parameter is optional.

STARTTime
: Specifies the time for the beginning of the window in which the storage rule is first processed. This parameter is optional. The storage rule runs daily within 5 minutes following the specified time.
Specify one of the following values:

Value	Description	Example
HH:MM:SS	A specific time.	23:30:08
NOW	The current time.	NOW
NOW+HH:MM or +HH:MM	The current time plus the specified number of hours and minutes.	NOW+02:00 or +02:00
NOW-HH:MM or -HH:MM	The current time minus the specified number of hours and minutes.	NOW-02:00 or -02:00

ACTIVE
: Specifies whether the storage rule processing occurs. This parameter is optional. The following values are possible:

  No
  : Specifies that the defined storage rule is inactive. The storage rule is not processed at the scheduled time.

  Yes
  : Specifies that the defined storage rule is active. The storage rule is processed at the scheduled time.

DESCription
: Specifies a description of the storage rule. This parameter is optional.

Update a storage rule

Update a storage rule that is named tieraction to move data from directory-container storage pools dirpool1 and dirpool2 to the cloud-container storage pool cloudpool1. Specify a start time of 23:30:08 hours and a maximum of 16 processes:

```
update stgrule tieraction srcpools=dirpool1,dirpool2
maxprocess=16 starttime=23:30:08
```

Related commands

Table 1. Commands related to UPDATE STGRULE

Command	Description
DEFINE STGRULE (tiering)	Defines a storage rule for tiering.
DELETE STGRULE	Deletes storage rules.
QUERY STGRULE	Displays storage rule information.

UPDATE VIRTUALFSMAPPING (Update a virtual file space mapping)

Use this command to update a virtual file space mapping definition.

Restriction: You cannot use the UPDATE VIRTUALFSMAPPING command to update a virtual file space mapping for an EMC Celerra or EMC VNX NAS device. You must use the DEFINE VIRTUALFSMAPPING command.

The NAS device needs an associated data mover definition because when the server updates a virtual file space mapping, the server contacts the NAS device to validate the virtual file system and file system name.

Privilege class

To issue this command, you must have one of the following privilege classes:

- System privilege
- Unrestricted policy privilege
- Restricted policy privilege for the domain to which the NAS node is assigned

Syntax

```
>>-UPDate VIRTUALFSMapping--node_name--virtual_filespace_name--->

>--+-------------------------------------+---------------------->
   '-FILESystem--=--new_file_system_name-'

>--+-----------------------------------------------------------+-><
   |                          .-NAMEType--=--SERVER----------. |
   '-PATH--=--new_path_name--+-------------------------------+-'
                             '-NAMEType--=--+-SERVER------+-'
                                            '-HEXadecimal-'
```

Parameters

node_name (Required)

Specifies the NAS node on which the file system and path reside. You cannot use wildcard characters or specify a list of names.

virtual_filespace_name (Required)

Specifies the virtual file space mapping to update. You cannot use wildcard characters or specify a list of names.

FILESystem

Specifies the new name of the file system in which the path is located. The file system name must exist on the specified NAS node. The file system name cannot contain wildcard characters. The file system name should only be modified when the file system name is modified on the NAS device or, for example, the directory is moved to a different file system. This parameter is optional.

PATH

Specifies the new path from the root of the file system to the directory. The path can only reference a directory. This should only be modified when the path on the NAS device has changed; for example, the directory is moved to a different path. The maximum length of the path is 1024 characters. The path name is case sensitive. This parameter is optional.

NAMEType

Specifies how the server should interpret the path name specified. Specify this parameter only if you specify a path. This parameter is useful when a path contains characters that are not part of the code page on which the server is running. The default value is SERVER.

Possible values are:

SERVER
: The code page in which the server is running is used to interpret the path.

HEXadecimal

The server interprets the path that you enter as the hexadecimal representation of the path. This option should be used when a path contains characters that cannot be entered. For example, this could occur if the NAS file system is set to a language different from the one in which the server is running.

Example: Modify the path of a virtual file space mapping

Update the virtual file space mapping named /mikeshomedir for the NAS node NAS1 by modifying the path.

```
update virtualfsmapping nas1 /mikeshomedir path=/new/home/mike
```

Related commands

Table 1. Commands related to UPDATE VIRTUALFSMAPPING

Command	Description
DEFINE VIRTUALFSMAPPING	Define a virtual file space mapping.
DELETE VIRTUALFSMAPPING	Delete a virtual file space mapping.
QUERY VIRTUALFSMAPPING	Query a virtual file space mapping.

UPDATE VOLHISTORY (Update sequential volume history information)

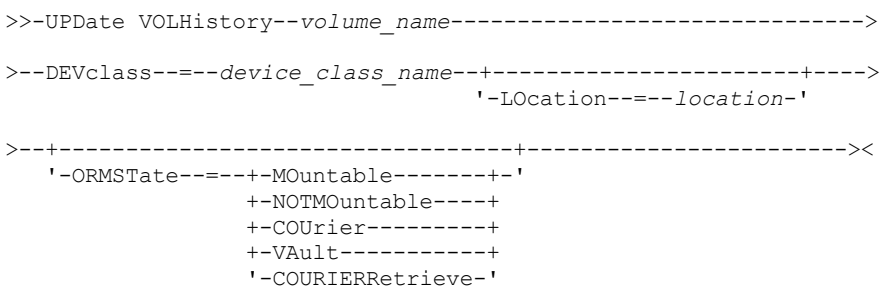
Use this command to update volume history information for a volume produced by a database backup or an export operation. This command does not apply to storage pool volumes.

Use the UPDATE BACKUPSET command to update specified backup set volume information in the volume history file. Do not use this UPDATE VOLHISTORY command to update backup set volume information in the volume history file.

Privilege class

You must have system privilege or unrestricted storage privilege to issue this command.

Syntax



Parameters

volume_name (Required)
: Specifies the volume name. The volume must have been used for a database backup or an export operation.

DEVclass (Required)
: Specifies the name of the device class for the volume.

LOcation
: Specifies the volume location. This parameter is required if the ORMSTATE parameter is not specified. The maximum text length is 255 characters. Enclose the text in quotation marks if it contains any blank characters.
Tip: The UPDATE VOLHISTORY command supports updates to the location information and ORMSTATE for snapshot database backup volumes.

ORMSTate
: Specifies a change to the state of a database backup volume. This parameter is required if the LOCATION parameter is not specified. This parameter is only supported for systems licensed with Disaster Recovery Manager. Possible states are:

MOuntable
: The volume contains valid data and is accessible for on-site processing.

NOTMOuntable
: The volume is on-site, contains valid data, and is not accessible for on-site processing.

COUrier
: The volume is being moved off-site.

VAult
: The volume is off-site, contains valid data, and is not accessible for on-site processing.

COURIERRetrieve
: The volume is being moved on-site.

Example: Update the location of a volume used for database backup

Update the location of a volume used for database backup, BACKUP1, to show that it has been moved to an off-site location.

```
update volhistory backup1 devclass=tapebkup
location="700 w. magee rd."
```

Related commands

Table 1. Commands related to UPDATE VOLHISTORY

Command	Description
BACKUP VOLHISTORY	Records volume history information in external files.
DELETE VOLHISTORY	Removes sequential volume history information from the volume history file.
MOVE DRMEDIA	Moves DRM media onsite and offsite.
PREPARE	Creates a recovery plan file.
QUERY DRMEDIA	Displays information about disaster recovery volumes.
QUERY VOLHISTORY	Displays sequential volume history information that has been collected by the server.

UPDATE VOLUME (Change a storage pool volume)

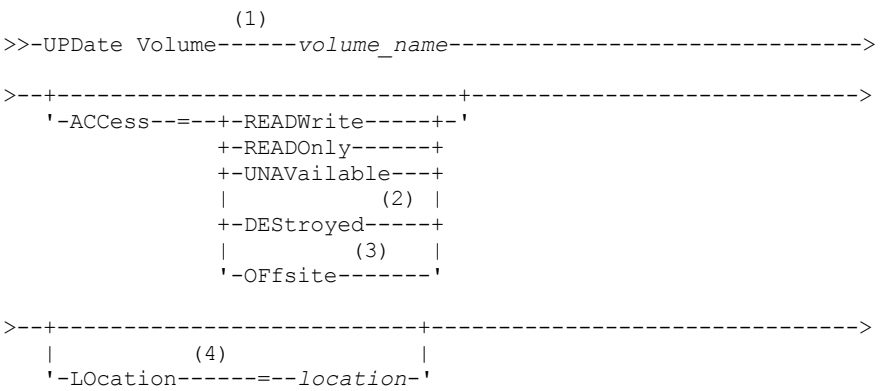
Use this command to change the access mode for one or more volumes in storage pools.

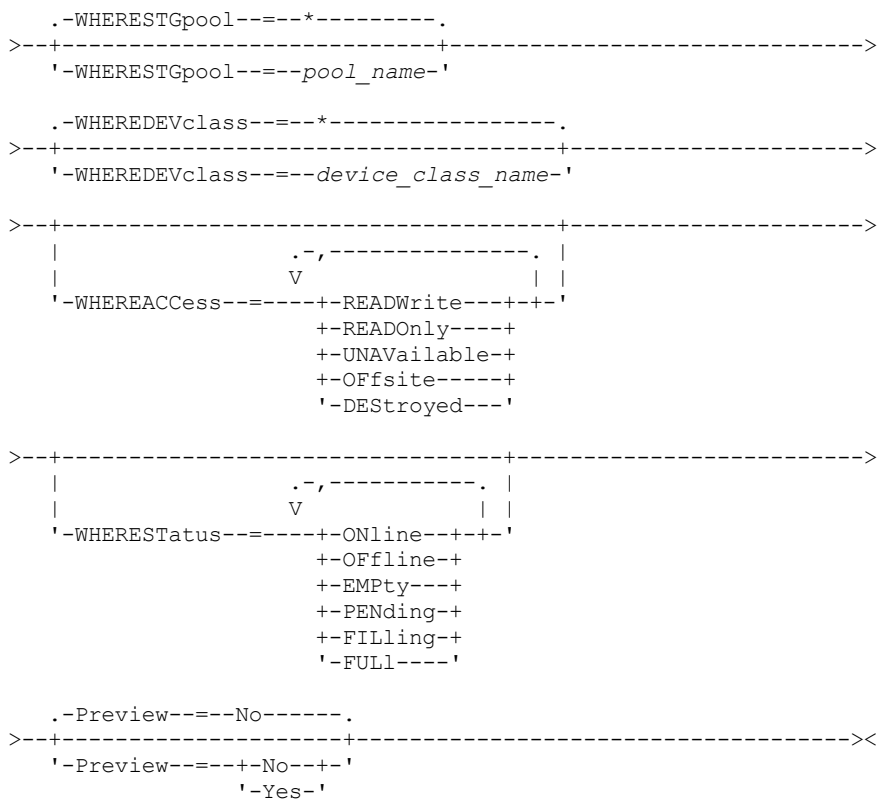
You can correct an error condition that is associated with a volume by updating the volume to an access mode of READWRITE. You can also use this command to change the location information for one or more volumes in sequential access storage pools.

Privilege class

To issue this command, you must have system privilege or operator privilege.

Syntax





Notes:

1. You must update at least one attribute (ACCESS or LOCATION).
2. This value is valid only for volumes in primary storage pools.
3. This value is valid only for volumes in copy, container-copy, and active-data storage pools.
4. This parameter is valid only for volumes in sequential access storage pools.

Parameters

volume_name (Required)
Specifies the storage pool volume to update. You can use wildcard characters to specify names.

ACCess
Specifies how client nodes and server processes (such as migration) can access files in the storage pool volume. This parameter is optional. Possible values are:

READWrite
Specifies that client nodes and server processes can read from and write to files stored on the volume.

If the volume that is being updated is an empty scratch volume that had an access mode of offsite, the server deletes the volume from the database.

READOnly
Specifies that client nodes and server processes can only read files that are stored on the volume.

If the volume that is being updated is an empty scratch volume that had an access mode of offsite, the server deletes the volume from the database.

UNAVailable
Specifies that neither client nodes nor server processes can access files that are stored on the volume.

Before making a random access volume unavailable, you must vary the volume offline. After you make a random access volume unavailable, you cannot vary the volume online.

If you make a sequential access volume unavailable, the server does not attempt to mount the volume.

If the volume that is being updated is an empty scratch volume that had an access mode of offsite, the server deletes the volume from the database.

DEStroyed
: Specifies that a primary storage pool volume has been permanently damaged. Neither client nodes nor server processes can access files that are stored on the volume. Use this access mode to indicate an entire volume that needs to be restored by using the RESTORE STGPOOL command. After all files on a destroyed volume are restored to other volumes, the server automatically deletes the destroyed volume from the database.

  Only volumes in primary storage pools can be updated to DESTROYED.

  Before you update a random access volume to DESTROYED access, you must vary the volume offline. After you update a random access volume to DESTROYED, you cannot vary the volume online.

  If you update a sequential access volume to DESTROYED, the server does not attempt to mount the volume.

  If a volume contains no files and you change the access mode to DESTROYED, the server deletes the volume from the database.

OFfsite
: Specifies that a copy, container-copy, or active-data storage pool volume is at an offsite location from which it cannot be mounted. Only volumes in copy, container-copy, or active-data storage pools can have the access mode of OFFSITE.

If you specify values for both the ACCESS and LOCATION parameters, but the access mode cannot be updated for a particular volume, the location attribute is also not updated for that volume. For example, if you specify ACCESS=OFFSITE and a LOCATION value for a primary storage pool volume, neither the access nor location values are updated because a primary storage pool volume cannot be given an access mode of OFFSITE.

LOcation
: Specifies the location of the volume. This parameter is optional. It can be specified only for volumes in sequential access storage pools. The maximum length of the location is 255 characters. Enclose the location in quotation marks if it contains any blank characters. To remove a previously defined location, specify the null string ("").

WHERESTGpool
: Specifies the name of the storage pool for volumes to be updated. Use this parameter to restrict the update by storage pool. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a storage pool name, volumes belonging to any storage pool are updated.

WHEREDEVclass
: Specifies the name of the device class for volumes to be updated. Use this parameter to restrict the update by device class. This parameter is optional. You can use wildcard characters to specify names. If you do not specify a device class name, volumes with any device class are updated.

WHEREACCess
: Specifies the current access mode of volumes to be updated. Use this parameter to restrict the update to volumes that currently have the specified access mode. This parameter is optional. You can specify multiple access modes by separating the modes with commas and no intervening spaces. If you do not specify a value for this parameter, the update is not restricted by the current access mode of a volume. Possible values are:

  READWrite
  : Update volumes with an access mode of READWRITE.

  READOnly
  : Update volumes with an access mode of READONLY.

  UNAVailable
  : Update volumes with an access mode of UNAVAILABLE.

  OFfsite
  : Update volumes with an access mode of OFFSITE.

  DEStroyed
  : Update volumes with an access mode of DESTROYED.

WHERESTatus
: Specifies the status of volumes to be updated. Use this parameter to restrict the update to volumes that have a specified status. This parameter is optional. You can specify multiple status values by separating the values with commas and no intervening spaces. If you do not specify a value for this parameter, the update is not restricted by volume status. Possible values are:

  ONline
  : Update volumes with a status of ONLINE.

  OFfline

Update volumes with a status of OFFLINE.

EMPty
: Update volumes with a status of EMPTY.

PENding
: Update volumes with a status of PENDING. These are volumes from which all files were deleted, but the time that is specified by the REUSEDELAY parameter has not elapsed.

FILling
: Update volumes with a status of FILLING.

FULl
: Update volumes with a status of FULL.

Preview
: Specifies whether you want to preview the update operation without updating volumes. This parameter is optional. The default value is NO. Possible values are:

  No
  : Specifies that volumes are updated.

  Yes
  : Specifies that you want only to preview the update operation. This option displays the volumes that will be updated if you run the update operation.

Example: Make a tape volume unavailable

Update a tape volume that is named DSMT20 to make it unavailable to client nodes and server processes.

```
update volume dsmt20 access=unavailable
```

Example: Update the access mode of all offsite volumes in a specific storage pool

Update all empty, offsite volumes in the TAPEPOOL2 storage pool. Set the access mode to READWRITE and delete the location information for the updated volumes.

```
update volume * access=readwrite location="" wherestgpool=tapepool2
    whereaccess=offsite wherestatus=empty
```

Related commands

Table 1. Commands related to UPDATE VOLUME

Command	Description
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.
DELETE VOLUME	Deletes a volume from a storage pool.
QUERY VOLUME	Displays information about storage pool volumes.
VARY	Specifies whether a disk volume is available to the server for use.

VALIDATE commands

Use the VALIDATE command to verify that an object is complete or valid for IBM Spectrum Protect™.

- Linux VALIDATE ASPERA (Validate an Aspera FASP configuration)
- AIX Linux Windows VALIDATE CLOUD (Validate cloud credentials)
- VALIDATE LANFREE (Validate LAN-Free paths)
- VALIDATE POLICYSET (Verify a policy set)
- VALIDATE REPLICATION (Validate replication for a client node)
- VALIDATE REPLPOLICY (Verify the policies on the target replication server)

Linux

VALIDATE ASPERA (Validate an Aspera FASP configuration)

Use this command to determine whether Aspera® Fast Adaptive Secure Protocol (FASP®) technology can be used to optimize data transfer in your system environment. Specifically, you can determine whether Aspera FASP technology would result in better network throughput than TCP/IP technology.

This command verifies the following additional items:

- Whether the system environment is correctly configured to use Aspera FASP technology
- Whether the required licenses for enabling Aspera FASP technology are installed

Aspera FASP technology is used to optimize data transfer for node replication or storage pool protection in a wide area network (WAN). However, you are not required to configure your system for node replication or storage pool protection to run the VALIDATE ASPERA command. If your system is configured for node replication or storage pool protection in a local environment, you can issue the command to evaluate whether the data can be successfully replicated to a remote server.

This command is available only on Linux x86_64 operating systems.

Before you issue the command, complete the following tasks:

1. Ensure that at least one server is defined in your system environment. Issue the PING SERVER command to ensure that you have connectivity to the defined server. For example, if the server is named VMRH6T, issue the following command:

   ```
   ping server vmrh6t
   ```

2. To use the VALIDATE ASPERA command to determine the speed of network throughput, install 30-day evaluation licenses or full, unlimited licenses on the source and target servers. For example, install licenses on the source and target servers, VMRH6 and VMRH6T. For instructions about obtaining and installing licenses, see Determining whether Aspera FASP technology can optimize data transfer in your system environment.

To simulate an environment that uses multiple sessions, you can run several instances of the VALIDATE ASPERA command simultaneously. If you plan to run multiple sessions, you might want to limit the bandwidth of each network connection to ensure that sufficient bandwidth is available for all network connections. To limit the bandwidth, specify the FASPTARGETRATE server option as described in FASPTARGETRATE.

You can query the current transferred amount by issuing the QUERY PROCESS command:

```
query process
```

You can obtain the process number from the output of the QUERY PROCESS command. You can cancel the process by issuing the CANCEL PROCESS command and specifying the process number, for example:

```
cancel process 3
```

Privilege class

Any administrator can issue this command.

Syntax

```
>>-VALidate ASPera--+-----------------------+----------------->
                    '---target_server_name---'

                              .-Wait--=--No------.
>--+-----------------------+--+------------------+-------------><
   '-DURation--=--seconds-'  '-Wait--=--+-No--+-'
                                        '-Yes-'
```

Parameters

target_server_name
: Specifies a previously defined server. This parameter is optional. To specify this parameter, follow the guidelines:

  - To determine whether Aspera FASP can optimize a node replication process, specify a target server that is configured for node replication.

- To determine whether Aspera FASP can optimize a storage pool protection process, specify a target server that is configured for storage pool protection.
- To determine whether Aspera FASP can optimize data transfer to a remote server that is defined but not configured for storage pool protection or node replication, specify that target server.
- If you do not specify a target server, the command output indicates whether the source server is correctly configured for Aspera FASP data transmission. The output also indicates whether a valid license for Aspera FASP is installed on the source server.

DURation
: Specifies the allotted time, in seconds, for transferring data across the network to evaluate throughput. This parameter is optional. The default value is 120 seconds. You can specify a value in the range 120 - 3600000 seconds. The allotted time is divided between the Aspera FASP and TCPIP data transfers.

Wait
: Specifies whether to wait for the server to complete the command processing. This parameter is optional. The default value is NO. You can specify one of the following values:

  No
  : Specifies that the server processes the command in the background. You can continue with other tasks while the command is being processed. If you specify NO, the output messages are displayed in the activity log.

  Yes
  : Specifies that the server processes the command in the foreground. The operation must complete processing before you can continue with other tasks. If you specify YES, the output messages are displayed in the administrative command-line client.
  Restriction: You cannot specify WAIT=YES from the server console.

Example: Display information about the status of an Aspera FASP configuration

On the source server, run the `VALIDATE ASPERA` command. To ensure that messages are displayed in the administrative command-line client, specify WAIT=YES. See Field descriptions for field descriptions.

```
validate aspera wait=yes
```

```
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.
Amount transferred using FASP: 0 MB per second. Amount transferred using
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: OK. Days until
license expires: Never.
```

Example: Verify whether the required licenses are installed

On the source server, run the `VALIDATE ASPERA` command and specify the target replication server. To ensure that messages are displayed in the administrative command-line client, specify WAIT=YES. See Field descriptions for field descriptions.

```
validate aspera vmrh6t wait=yes
```

```
ANR0984I Process 8 for VALIDATE ASPERA started in the FOREGROUND at 09:35:21 AM.
ANR3672E The license file that is required to enable Aspera Fast Adaptive
Secure Protocol (FASP) technology was not found on the VMRH6 server.
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.
Amount transferred using FASP: 0 MB per second. Amount transferred using
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: Invalid
configuration. Days until license expires: Expired.
ANR0985I Process 8 for VALIDATE ASPERA running in the FOREGROUND completed with
completion state FAILURE at 09:35:21 AM.
ANR1893E Process 8 for VALIDATE ASPERA completed with a completion state of
FAILURE.
```

Field descriptions

Status
: The status of the configuration. The following values are possible:

- `OK` indicates that no issues are detected.
- `Invalid configuration` indicates that a configuration file, license file, or Aspera FASP library file is missing.
- `License issue` indicates that a license is missing, invalid, or expired.

- `Server failure` indicates that all ports are in use, a network read/write error occurred, or the Aspera FASP log file is unwritable.
- `Invalid target configuration` indicates that a configuration file, license file, or Aspera FASP library file is missing on the target server.
- `Failure on target server` indicates that all ports are in use, a network read/write error occurred, or the Aspera FASP log file is unwritable.
- `License issue on target server` indicates that a license is invalid or expired on the target server.
- `Unsupported operating system` indicates that an operating system other than Linux x86_64 is installed on one or both servers.
- `Unknown` indicates that an unexpected error occurred. To identify the error, review the log messages.

Days until license expires
: The following values are possible:

- `Never` indicates that a full, unlimited license is installed.
- `Today` indicates that a 30-day evaluation license is installed and it expires today.
- `Expired` indicates that a 30-day evaluation license is installed, but has expired.
- *Number* indicates that a 30-day evaluation license is installed and will expire in the specified number of days.
- `License not found` indicates that no license was found.

Amount transferred using TCP/IP
: The speed of data transfer, in megabytes per second, using TCP/IP technology.

Amount transferred using FASP
: The speed of data transfer, in megabytes per second, using Aspera FASP technology.

Latency
: The latency of data transfer in microseconds.

Related commands

Table 1. Commands related to VALIDATE ASPERA

Command	Description
CANCEL SESSION	Cancels active sessions with the server.
DEFINE SERVER	Defines a server for server-to-server communications.
PING SERVER	Tests the connections between servers.
AIX Linux Windows PROTECT STGPOOL	AIX Linux Windows Protects a directory-container storage pool.
REPLICATE NODE	Replicates data in file spaces that belong to a client node.

VALIDATE CLOUD (Validate cloud credentials)

Before you define a storage pool, use this command to ensure that the credentials for a cloud-container storage pool are valid and that the necessary permissions are granted to the user.

Privilege class

Any administrator can issue this command.

Syntax

```
                  .-CLOUDType--=--SWift-------------.
>>-VALidate CLOud--+-----------------------------------+---------->
                   '-CLOUDType--=--+-AZure---------+-'
                                   +-S3------------+
                                   +-IBMCLoudswift-+
                                   +-SWift---------+
                                   '-V1Swift-------'

                                                    (1)
>--CLOUDUrl--=--cloud_url--IDentity--=--cloud_identity---------->
```

```
>--PAssword--=--password--+-------------------------------+--><
                         |                           (2) |
                         '-BUCKETName--=--bucket_name-----'
```

Notes:

1. If you specify CLOUDTYPE=AZURE, do not specify the IDENTITY parameter.
2. The BUCKETNAME parameter is valid only if you specify CLOUDTYPE=S3.

Parameters

CLOUDType
: Specifies the type of cloud environment where you are configuring the storage pool.
You can specify one of the following values:

  AZure
  : Specifies that the storage pool uses a Microsoft Azure cloud computing system.

  S3
  : Specifies that the storage pool uses a cloud computing system with the Simple Storage Service (S3) protocol, such as IBM® Cloud Object Storage or Amazon Web Services (AWS) S3.

  IBMCloudswift
  : Specifies that the storage pool uses an IBM Cloud cloud computing system with an OpenStack Swift cloud computing system.

  SWift
  : Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 2 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol that it is using.

  V1Swift
  : Specifies that the storage pool uses an OpenStack Swift cloud computing system. This value also specifies that the storage pool uses Version 1 of the protocol for authentication to the cloud. The URL of the cloud usually contains the version number of the protocol that it is using.

  This parameter is optional. If you do not specify the parameter, the default value, SWIFT, is used.

CLOUDUrl (Required)
: Specifies the URL of the cloud environment where you configure the storage pool. Based on your cloud provider, you can use a blob service endpoint, region endpoint URL, an accesser IP address, a public authentication endpoint, or a similar value for this parameter. Ensure that you include the protocol, such as `https://` or `http://`, at the beginning of the URL. The maximum length of the web address is 870 characters. The CLOUDURL parameter is validated when the first backup begins.

IDentity (Required)
: Specifies the user ID for the cloud. This parameter is required for all supported cloud computing systems except Azure. If you specify CLOUDTYPE=AZURE, do not specify the IDENTITY parameter. Based on your cloud provider, you can use an access key ID, a user name, a tenant name and user name, or a similar value for this parameter. The maximum length of the user ID is 255 characters.

PAssword (Required)
: Specifies the password for the cloud. Based on your cloud provider, you can use a shared access signature (SAS) token, secret access key, an API key, a password, or a similar value for this parameter. This parameter is required. The maximum length of the password is 255 characters.

BUCKETName
: Specifies the name for an AWS S3 bucket or a IBM Cloud Object Storage vault to use with this storage pool, instead of using the default bucket name or vault name. This parameter is optional, and is valid only if you specify CLOUDTYPE=S3. If a bucket or vault exists with the name that you specify, that bucket or vault is tested to ensure that the proper permissions are set. If the bucket or vault does not exist, the parameter verifies only that a bucket or vault with that name does not exist. Follow the naming restrictions for your cloud provider when you specify this parameter. Review the permissions for the bucket or vault and make sure that the credentials have permission to read, write, list, and delete objects in this bucket or vault.
  Tip: If you do not specify the BUCKETNAME parameter, the Replication Globally Unique ID is used as the default bucket name. The default is

  `ibmsp` *guid*

where *guid* is the REPLICATION GLOBALLY UNIQUE ID value, minus the periods, in the output of the QUERY REPLSERVER command. For example, if the Replication Globally Unique ID is 52.82.39.20.64.d0.11.e6.9d.77.0a.00.27.00.00.00, the default bucket name is ibmsp.5282392064d011e69d770a0027000000.

Example: Verify the credentials of an S3 cloud-container storage pool

Validate the credentials of the cloud-container storage pool.

```
validate cloud
cloudtype=s3 cloudurl=http://123.234.123.234:5000/v2.0
password=protect8991 bucketname=ibmsp.5282392064d011e69d770a0027000000
```

Related commands

Table 1. Commands related to VALIDATE CLOUD

Command	Description
DEFINE STGPOOL (cloud-container)	Define a cloud-container storage pool.
QUERY REPLSERVER	Displays information about replicating servers.
UPDATE STGPOOL (cloud-container)	Update a cloud-container storage pool.

VALIDATE LANFREE (Validate LAN-Free paths)

Use this command to determine which destinations for a given node using a specific storage agent are capable of LAN-Free data movement.

Privilege class

To issue this command, you must have system privilege.

Syntax

```
>>-VALidate LAnfree--node_name--stgagent_name------------------><
```

Parameters

node_name (Required)
: The name of the node to evaluate.

stgagent_name (Required)
: The name of the storage agent to evaluate.

Example: Validate a current LAN-Free configuration

Validate the current server definitions and configuration for node TIGER to use storage agent AIX_STA1 for LAN-free data operations.

```
validate lanfree tiger aix_sta1

Node  Storage  Operation Mgmt Class Destination LAN-Free Explanation
Name  Agent              Name       Name        capable?
----- -------- --------- ---------- ----------- -------- -----------
TIGER AIX_STA1 BACKUP    STANDARD   OUTPOOL     NO       No available
                                                         online paths.
TIGER AIX_STA1 BACKUP    STANDARD   PRIMARY     NO       Destination
                                                         storage pool
                                                         is configured
                                                         for simultan-
                                                         eous write.
TIGER AIX_STA1 BACKUP    STANDARD   SHRPOOL     YES
TIGER AIX_STA1 BACKUP    NOARCH     LFFILE      NO       Storage pool
                                                         contains data
```

```
                                                    deduplicated
                                                    by clients,
                                                    and is not
                                                    accessible by
                                                    storage
                                                    agents V6.1
                                                    or earlier.
TIGER AIX_STA1 ARCHIVE   STANDARD   OUTPOOL     NO  No available
                                                    online paths.
TIGER AIX_STA1 ARCHIVE   STANDARD   PRIMARY     NO  Destination
                                                    storage pool
                                                    is configured
                                                    for simultan-
                                                    eous write.
TIGER AIX_STA1 ARCHIVE   STANDARD   SHRPOOL     YES
```

Related commands

Table 1. Commands related to VALIDATE LANFREE

Command	Description
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY DEVCLASS	Displays information about device classes.
QUERY DOMAIN	Displays information about policy domains.
QUERY DRIVE	Displays information about drives.
QUERY LIBRARY	Displays information about one or more libraries.
QUERY MGMTCLASS	Displays information about management classes.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY PATH	Displays information about the path from a source to a destination.
QUERY POLICYSET	Displays information about policy sets.
QUERY SERVER	Displays information about servers.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.
QUERY STGPOOL	Displays information about storage pools.

VALIDATE POLICYSET (Verify a policy set)

Use this command to verify that a policy set is complete and valid before you activate it. The command examines the management class and copy group definitions in the policy set and reports on conditions that you need to consider before activating the policy set.

The VALIDATE POLICYSET command fails if any of the following conditions exist:

- The policy set has no default management class.
- A copy group within the policy set specifies a copy storage pool as a destination.
- A management class specifies a copy storage pool as the destination for files that were migrated by an IBM Spectrum Protect™ for Space Management client.
- A TOCDESTINATION parameter is specified, and the storage pool is either a copy pool or has a data format other than NATIVE or NONBLOCK.

The server issues warning messages for the following conditions:

- A copy group specifies a storage pool that does not exist as a destination for backed-up or archived files.

  If you activate a policy set with copy groups that specify nonexistent storage pools, the client backup or archive operations fail.

- A management class specifies a storage pool that does not exist as a destination for files migrated by IBM Spectrum Protect for Space Management clients.
- The policy set does not have one or more management classes that exist in the current ACTIVE policy set.

  If you activate the policy set, backup files bound to the deleted management classes are rebound to the default management class in the new active policy set.

- The policy set does not have one or more copy groups that exist in the current ACTIVE policy set.

  If you activate the policy set, files bound to the management classes with deleted copy groups are no longer archived or backed up.

- The default management class for the policy set does not contain a backup or archive copy group.

  If you activate the policy set with this default management class, clients using the default cannot back up or archive files.

- A management class specifies that a backup version must exist before a file can be migrated from a client node (MIGREQUIRESBKUP=YES), but the management class does not contain a backup copy group.

If the server has data retention protection enabled, the following conditions must exist:

- All management classes in the policy set to be validated must contain an archive copy group.
- If a management class exists in the active policy set, a management class with the same name must exist in the policy set to be validated.
- If an archive copy group exists in the active policy set, the corresponding copy group in the policy set to be validated must have a RETVER value at least as large as the corresponding values in the active copy group.

Privilege class

To issue this command, you must have system privilege, unrestricted policy privilege, or restricted policy privilege for the policy domain to which the policy set belongs.

Syntax

```
>>-VALidate POlicyset--domain_name--policy_set_name------------><
```

Parameters

domain_name (Required)
: Specifies the name of the policy domain to which the policy set is assigned.

policy_set_name (Required)
: Specifies the name of the policy set to be validated.

Example: Validate a specific policy set

Validate the policy set `VACATION` located in the `EMPLOYEE_RECORDS` policy domain.

```
validate policyset employee_records vacation
```

Related commands

Table 1. Commands related to VALIDATE POLICYSET

Command	Description
ACTIVATE POLICYSET	Validates and activates a policy set.
COPY POLICYSET	Creates a copy of a policy set.
DEFINE COPYGROUP	Defines a copy group for backup or archive processing within a specified management class.
DEFINE MGMTCLASS	Defines a management class.

Command	Description
DELETE POLICYSET	Deletes a policy set, including its management classes and copy groups, from a policy domain.
QUERY POLICYSET	Displays information about policy sets.
UPDATE COPYGROUP	Changes one or more attributes of a copy group.
UPDATE POLICYSET	Changes the description of a policy set.

VALIDATE REPLICATION (Validate replication for a client node)

Use this command to identify the replication rules that apply to file spaces in client nodes that are configured for replication. You can also use this command to verify that the source replication server can communicate with the target replication server.

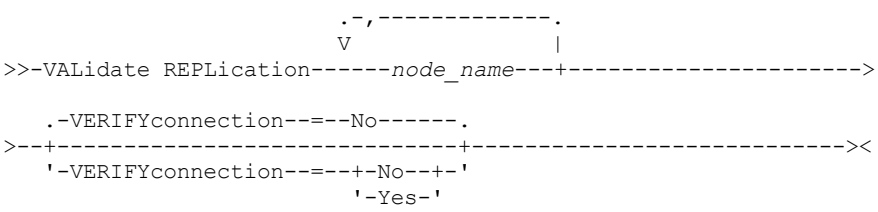
Before you begin replication processing, use the VALIDATE REPLICATION command to determine whether your replication configuration is correct.

Issue this command on the server that acts as a source for replicated data.

Privilege class

To issue this command, you must have system privilege.

Syntax



Parameters

node_name (Required)
: Specifies the name of the client node whose file spaces you want to display. To specify multiple client node names, separate the names with commas and no intervening spaces. You can use wildcard characters to specify names.

  Information is displayed only for client nodes that are either enabled or disabled for replication. The replication mode must be SEND. To determine whether a client node is enabled or disabled for replication and its mode, issue the QUERY NODE command. Look for values in the Replication State and Replication Mode fields.

VERIFYconnection
: Specifies whether to check the connection to a target replication server. The version of the target replication server is also checked to verify that it is Version 6.3 or later. This parameter is optional. The default is NO. You can specify one of the following values:

  No
  : The connection and version of the target replication server are not checked.

  Yes
  : The connection and version of the target replication server are checked.

Example: Validate replication for a client node

The name of the client node is NODE1. Verify the connection status between the source and the target replication servers.

```
validate replication node1 verifyconnection=yes

                 Node Name: NODE1
           Filespace Name: \\node1\c$
```

```
                      FSID: 1
                      Type: Bkup
Controlling Replication Rule: ACTIVE_DATA
      Replication Rule Level: System Level
                 Server Name: DRSRV
           Connection Status: Valid Connection

                 Node Name: NODE1
            Filespace Name: \\node1\c$
                      FSID: 1
                      Type: Arch
Controlling Replication Rule: ALL_DATA_HIGH_PRIORITY
      Replication Rule Level: Node Level
                 Server Name: DRSRV
           Connection Status: Valid Connection

                 Node Name: NODE1
            Filespace Name: \\node1\c$
                      FSID: 1
                      Type: SpMg
Controlling Replication Rule: ALL_DATA
      Replication Rule Level: System Level
                 Server Name: DRSRV
           Connection Status: Valid Connection
```

Output is displayed for all data types regardless of whether a file space contains the data types. For example, if a file space contains only backup and archive data, the output of the VALIDATE REPLICATION command also contains information that would be relevant to space-managed data.

Field descriptions

Node Name
: The node that owns the replicated data.

Filespace Name
: The name of the file space that belongs to the node.

  File space names can be in a different code page or locale than the server. If they are, the names in the Operations Center and the administrative command-line interface might not be displayed correctly. Data is backed up and can be restored normally, but the file space name or file name might be displayed with a combination of invalid characters or blank spaces.

  If the file space name is Unicode-enabled, the name is converted to the server code page for display. The success of the conversion depends on the operating system, the characters in the name, and the server code page. Conversion can be incomplete if the string includes characters that are not available in the server code page or if the server cannot access system conversion routines. If the conversion is incomplete, the name might contain question marks, blanks, unprintable characters, or ellipses (...).

FSID
: The file space identifier for the file space. The server assigns a unique FSID when a file space is first stored on the server.

Type
: The type of data. The following values are possible:

  Arch
  : Archive data

  Bkup
  : Backup data

  SpMg
  : Data that was migrated by an IBM Spectrum Protect™ for Space Management client.

Controlling Replication Rule
: The name of the replication rule that controls replication for a data type in a file space. To determine whether the controlling rule is a file space rule, a client rule, or a server rule, check the Replication Rule Level field.

Replication Rule Level
: The level of the controlling rule in the replication-rule hierarchy. The following values are possible:

  Filespace
  : The controlling rule is assigned to a data type in the file space.

  Node

The controlling rule is assigned to a data type for a client node.

Server
The controlling rule is assigned to a data type for all file spaces in all client nodes that are configured for replication.

Server Name
The name of the target replication server to be queried.

Connection Status
The connection status between the source and the target replication server. The following values are possible:

Valid Connection
Communication with the target replication server was successful, and the target replication server is a V6.3 server.

Target Server Not Set
The target replication server is not set. To set the target replication server, issue the SET REPLSERVER command.

Communication Failure
The source replication server was unable to contact the target replication server. Examine the activity log for error messages about failed communications. Consider the following possible causes:

- The replication configuration on the source replication server is not valid. One or more of the following problems might exist:
  - The server definition for the target replication server is incorrect.
  - If the target replication-server definition was deleted and redefined, issue the PING SERVER command to test the connection between the source and the target replication server. If the PING SERVER command is successful, issue the UPDATE SERVER command and specify FORCESYNC=YES to reset the server verification keys.
  - The server name, server low-level address, server high-level address, and server password do not match the values that are specified in the server definition on the target replication server.
- The replication configuration on the target replication server is not valid. One or more of the following problems might exist:
  - The version of the target replication server is earlier than V6.3.
  - The server definition for the source replication server is incorrect.
  - The server name, server low-level address, server high-level address, and server password do not match the values that are specified in the server definition on the source replication server.
- Network communications are unavailable. To test the connection between the source and target server, issue the PING SERVER command.
- The target replication server is unavailable.
- Sessions between the source and the target replication servers are disabled. To verify the status of sessions, issue the QUERY STATUS command.

Replication Suspended
Replication processing is suspended when you restore the database on the source replication server or you disable replication processing on this server by issuing the DISABLE REPLICATION command.

Related commands

Table 1. Commands related to VALIDATE REPLICATION

Command	Description
DISABLE REPLICATION	Prevents outbound replication processing on a server.
ENABLE REPLICATION	Allows outbound replication processing on a server.
ENABLE SESSIONS	Resumes server activity following the DISABLE command or the ACCEPT DATE command.
QUERY FILESPACE	Displays information about data in file spaces that belong to a client.
QUERY NODE	Displays partial or complete information about one or more clients.
QUERY REPLRULE	Displays information about node replication rules.
QUERY SERVER	Displays information about servers.
QUERY STATUS	Displays the settings of server parameters, such as those selected by the SET commands.

Command	Description
REPLICATE NODE	Replicates data in file spaces that belong to a client node.
SET ARREPLRULEDEFAULT	Specifies the server node-replication rule for archive data.
SET BKREPLRULEDEFAULT	Specifies the server node-replication rule for backup data.
SET REPLSERVER	Specifies a target replication server.
SET SPREPLRULEDEFAULT	Specifies the server node-replication rule for space-managed data.
UPDATE FILESPACE	Changes file-space node-replication rules.
UPDATE NODE	Changes the attributes that are associated with a client node.
UPDATE REPLRULE	Enables or disables replication rules.
UPDATE SERVER	Updates information about a server.

VALIDATE REPLPOLICY (Verify the policies on the target replication server)

Use this command to compare the policies for client nodes on the source replication server with the same policies on the target replication server where the client node data is being replicated.

The command displays the differences between these policies so that you can verify that any differences between the policies on the source and target replication servers are intended or you can modify the policies on the target replication server.

Ensure that IBM Spectrum Protect™, Version 7.1.1 or later, is installed on the source and target replication servers before you issue this command. Issue this command on the source replication server.

Privilege class

Any administrator can issue this command.

Syntax

```
>>-VALidate REPLPolicy--+-------------+------------------------><
                        '-server_name-'
```

Parameters

server_name
: Specifies the name of the target replication server that has policies you want to verify. This parameter is optional. If you do not specify this parameter, the command sets the default replication server as the target replication server.

Example: Display the differences between the replication policies on a source and target replication server

To display the differences between the policies on the source replication server and the policies on the target replication server, CVTCVS_LXS_SRV2, where the client data is replicated, issue the following command on the source replication server:

```
VALIDATE REPLPOLICY CVTCVS_LXS_SRV2

Policy domain name          Policy domain name      Target
on this server              on target server        server name
--------------------------  ----------------------  -----------------
STANDARD                    STANDARD                CVTCVS_LXS_SRV2

Differences in policy set:
Change detected             Source server value     Target server value
--------------------------  ----------------------  -----------------
Mgmt class only on target   Not applicable          STANDARD2
```

```
Mgmt Class only on source   STANDARD1               Not applicable

Differences in backup       STANDARD in             STANDARD
copy group                  management class
Change detected             Source server value     Target server value
--------------------------  ----------------------  ------------------
Versions data exists        2                       20


Affected nodes
-----------------------------------------------------------------------
NODE1,NODE2,NODE3,NODE4,NODE5
```

Field descriptions

Policy domain name on this server
: Specifies the policy domain name on the source replication server where the command is issued.

Policy domain name on target server
: Specifies the policy domain name on the target replication server.

Target server name
: Specifies the name of the target replication server.

Differences in policy set:
: Specifies the differences between the policies that are defined on the source and target replication servers. The differences between the policies are listed under the following fields:

  Change detected
  : Specifies the list of policy items that are different between the source and target replication servers.

  Source server value
  : Specifies the value for the policy item on the source replication server.

  Target server value
  : Specifies the value for the policy item on the target replication server.

Differences in backup copy group <backup_copy_group_name> in default management class OR Differences in archive copy group <archive_copy_group_name> in default management class
: Specifies the differences between the backup copy group or the archive copy group in the management class. The differences are listed under the following fields:

  Change Detected
  : Specifies the list of copy group fields that are different.

  Source server value
  : Specifies the value in the copy group field on the source replication server.

  Target server value
  : Specifies the value in the copy group field on the target replication server.

Affected nodes
: Specifies the names of all the client nodes that are affected by the changes that are shown in this output.

Related commands

Table 1. Commands related to VALIDATE REPLPOLICY

Command	Description
VALIDATE REPLICATION	Verifies replication for file spaces and data types.
QUERY REPLSERVER	Displays information about replicating servers.
SET DISSIMILARPOLICIES	Enable the policies on the target replication server to manage replicated data.
QUERY DOMAIN	Displays information about policy domains.
QUERY POLICYSET	Displays information about policy sets.
QUERY COPYGROUP	Displays the attributes of a copy group.
QUERY MGMTCLASS	Displays information about management classes.

VARY (Bring a random access volume online or offline)

Use this command to make a random access storage pool volume online or offline to the server.

Privilege class

This command is valid only for volumes on random access devices. For example, use this command during maintenance or corrective action of a random access volume. You cannot vary a random access volume online that is defined as unavailable.

To issue this command, you must have system privilege or operator privilege.

Syntax

```
                                  .-Wait--=--No------.
>>-VARy--+-ONline--+--volume_name--+------------------+--------><
         '-OFfline-'                '-Wait--=--+-No--+-'
                                               '-Yes-'
```

Parameters

ONline
: Specifies that the server can use the random access volume.

OFfline
: Specifies that the server cannot use the volume.

volume_name (Required)
: Specifies the volume identifier. Volume names cannot contain embedded blanks or equal signs.

Wait
: Specifies whether to wait for the server to complete processing this command in the foreground. This parameter is optional. The default is NO. Possible values are:

  No
  : Specifies that the server processes this command in the background, while other tasks run. The server displays messages created from the background process either in the activity log or the server console, depending on where messages are logged.

  Yes
  : Specifies that the server processes this command in the foreground. Wait for the command to complete before you continue with other tasks. The server displays the output messages to the administrative client when the command completes.

    AIX Linux Windows You cannot specify WAIT=YES from the server console.

Example: Bring volume online

AIX Linux Make volume /adsm/stgvol/1 available to the server for use as a storage pool volume. AIX Linux

```
vary online /adsm/stgvol/1
```

Windows Make volume j:\storage\pool001 available to the server for use as a storage pool volume. Windows

```
vary online j:\storage\pool001
```

Related commands

Table 1. Commands related to VARY

Command	Description
CANCEL PROCESS	Cancels a background server process.
DEFINE VOLUME	Assigns a volume to be used for storage within a specified storage pool.

Command	Description
DELETE VOLUME	Deletes a volume from a storage pool.
QUERY PROCESS	Displays information about background processes.
QUERY VOLUME	Displays information about storage pool volumes.

Server options

At installation, IBM Spectrum Protect™ provides a server options file that contains a set of default options to start the server.

The file is:

- dsmserv.opt in the server instance directory

Server options let you customize the following:

- Communication
- Server storage
- Client-server
- Date, number, time, and language
- Database and recovery log
- Data transfer
- Message
- Event logging
- Security and licensing

Several other options are available for miscellaneous purposes. These undocumented options are intended to be used only by IBM® support.
To display the current option settings, enter:

```
query option
```

- Modifying server options
  The server reads the server options file at server initialization. When you update a server option by editing the file, you must stop and start the server to activate the updated server options file.
- Types of server options
  Server options let you customize how some functions and processes work.
- 3494SHARED
  The 3494SHARED option specifies whether an IBM 3494 library can share applications other than IBM Spectrum Protect.
- ACSACCESSID
  The ACSACCESSID option specifies the ID for the ACS access control for an ACSLS library.
- ACSLOCKDRIVE
  The ACSLOCKDRIVE option specifies if the drives within the ACSLS libraries are locked. Drive locking ensures the exclusive use of the drive in the ACSLS library in a shared environment. However, there is some performance gain if libraries are not locked. When other applications do not share the IBM Spectrum Protect drives, drive locking is not required.
- ACSQUICKINIT
  The ACSQUICKINIT option specifies whether, at server startup, the initialization of the ACSLS library is a quick or full initialization. The default is Yes. A quick initialization avoids the overhead associated with synchronizing the IBM Spectrum Protect server inventory with the ACSLS library inventory (through an audit of the library).
- ACSTIMEOUTX
  The ACSTIMEOUTX option specifies the multiple for the built-in timeout value for ACSLS APIs. The built-in timeout value for the ENTER, EJECT, and AUDIT ACS API is 1800 seconds; for all other ACSLS APIs it is 600 seconds. For example, if the multiple value specified is 5, the timeout value for audit API becomes 9000 seconds, and all other APIs become 3000 seconds.
- ACTIVELOGDIRECTORY
  The ACTIVELOGDIRECTORY option specifies the name of the directory where all active logs are stored.
- ACTIVELOGSIZE
  The ACTIVELOGSIZE option sets the total log size.
- ADMINCOMMTIMEOUT
  The ADMINCOMMTIMEOUT option specifies how long the server waits for an expected administrative client message during an operation that causes a database update.

- ADMINIDLETIMEOUT
  The ADMINIDLETIMEOUT option specifies the amount of time, in minutes, that an administrative client session can be idle before the server cancels the session.
- ADMINONCLIENTPORT
  The ADMINONCLIENTPORT option specifies whether the TCPPORT can be used by administrative sessions. The default is YES.
- Windows ADSMGROUPNAME
  The ADSMGROUPNAME option specifies the name of a Windows group. A client node must be a member of this group to use the IBM Spectrum Protect server through NT Unified Logon. The client node must also be a registered IBM Spectrum Protect client node.
- ALIASHALT
  The ALIASHALT option allows administrators to give the IBM Spectrum Protect **HALT** command a different name.
- ALLOWDESAUTH
  The ALLOWDESAUTH option specifies whether to allow use of the Data Encryption Standard (DES) algorithm for authentication between a server and a backup-archive client.
- ALLOWREORGINDEX
  The ALLOWREORGINDEX option specifies whether server-initiated index reorganization is enabled or disabled.
- ALLOWREORGTABLE
  The ALLOWREORGTABLE option specifies whether server-initiated table reorganization is enabled or disabled.
- ARCHFAILOVERLOGDIRECTORY
  The ARCHFAILOVERLOGDIRECTORY option specifies the directory which the server uses to store archive log files that cannot be stored in the archive log directory.
- ARCHLOGCOMPRESS
  You can enable or disable compression of archive logs on the IBM Spectrum Protect server. By compressing the archive logs, you reduce the amount of space that is required for storage.
- ARCHLOGDIRECTORY
  The ARCHLOGDIRECTORY option specifies a directory that the database manager can archive a log file into after all the transactions represented in that log file are completed.
- ARCHLOGUSEDTHRESHOLD
  The ARCHLOGUSEDTHRESHOLD option specifies when to start an automatic database backup in relation to the percentage of archive log file space used. The default is 80 percent.
- ASSISTVCRRECOVERY
  The ASSISTVCRRECOVERY option specifies whether IBM Spectrum Protect assists an IBM 3590 drive in recovering from a lost or corrupted Vital Cartridge Records (VCR) condition. If you specify YES (the default) and if IBM Spectrum Protect detects an error during the mount processing, it locates to the end-of-data during the dismount processing to allow the drives to restore the VCR. During the tape operation, there might be some small effect on performance because the drive cannot complete a fast locate with a lost or corrupted VCR. However, there is no loss of data.
- AUDITSTORAGE
  As part of a license audit operation, the server calculates, by node, the amount of server storage used for backup, archive, and space–managed files. For servers managing large amounts of data, this calculation can take a great deal of CPU time and can stall other server activity. You can use the AUDITSTORAGE option to specify that storage is not to be calculated as part of a license audit.
- BACKUPINITIATIONROOT
  The BACKUPINITIATIONROOT option specifies whether the server overrides node parameter values for users who are not IBM Spectrum Protect authorized users.
- CHECKTAPEPOS
  The CHECKTAPEPOS option specifies whether the IBM Spectrum Protect server validates the position of data blocks on tape.
- CLIENTDEDUPTXNLIMIT
  The CLIENTDEDUPTXNLIMIT option specifies the maximum size of a transaction when client-side deduplicated data is backed up or archived.
- CLIENTDEPLOYCATALOGURL
  The CLIENTDEPLOYCATALOGURL option specifies the location of the catalog file that is used for automatic client deployment operations.
- CLIENTDEPLOYUSELOCALCATALOG
  The CLIENTDEPLOYCATALOGURL option specifies whether the local version of the catalog file is used for automatic client deployment operations.
- COMMMETHOD
  The COMMMETHOD option specifies a communication method to be used by the server.
- COMMTIMEOUT
  The COMMTIMEOUT option specifies how long the server waits for an expected client message during an operation that causes a database update. If the length of time exceeds this time-out, the server ends the session with the client. You may

want to increase the time-out value to prevent clients from timing out. Clients may time out if there is a heavy network load in your environment or they are backing up large files.

- CONTAINERRESOURCETIMEOUT
  The CONTAINERRESOURCETIMEOUT option specifies how long the server waits to complete a data store operation to a container storage pool.
- Windows DATEFORMAT
  The DATEFORMAT option specifies the format in which dates are displayed by the server.
- DBDIAGLOGSIZE
  This option helps to control the amount of space that is used by diagnostic log files.
- DBDIAGPATHFSTHRESHOLD
  The DBDIAGPATHFSTHRESHOLD option specifies the threshold for free space on the file system or disk that contains the db2diag.log file.
- DBMEMPERCENT
  Use this option to specify the percentage of the virtual address space that is dedicated to the database manager processes.
- DBMTCPPORT
  The DBMTCPPORT option specifies the port number on which the TCP/IP communication driver for the database manager waits for requests for client sessions.
- DEDUPREQUIRESBACKUP
  The DEDUPREQUIRESBACKUP option specifies whether volumes in primary sequential-access storage pools that are set up for data deduplication can be reclaimed and whether duplicate data can be discarded before the storage pools are backed up.
- DEDUPTIER2FILESIZE
  The DEDUPTIER2FILESIZE option specifies at what file size IBM Spectrum Protect begins to use Tier 2 data deduplication.
- DEDUPTIER3FILESIZE
  The DEDUPTIER3FILESIZE option specifies at what file size IBM Spectrum Protect begins to use Tier 3 data deduplication.
- DEVCONFIG
  The DEVCONFIG option specifies the name of a file in which you want IBM Spectrum Protect to store a backup copy of device configuration information.
- DISABLEREORGTABLE
  The DISABLEREORGTABLE option specifies whether online table reorganization is disabled for table names that are specified in the tables list.
- DISABLESCHEDS
  The DISABLESCHEDS option specifies whether administrative and client schedules are disabled during IBM Spectrum Protect server recovery.
- DISPLAYLFINFO
  The DISPLAYLFINFO option specifies how the accounting records and summary table entries report the node name.
- DNSLOOKUP
  The DNSLOOKUP option specifies whether the server uses system API calls to determine the domain name server (DNS) names of systems that contact the server.
- DRIVEACQUIRERETRY
  The DRIVEACQUIRERETRY option lets you specify how many times the server retries the acquisition of a drive in an IBM 349x library. If the library is shared among multiple applications, its drives may appear to be available to the server (through the use of a background polling process) when they are not.
- ENABLENASDEDUP
  The ENABLENASDEDUP server option specifies whether the server deduplicates data that is stored by a network-attached storage (NAS) file server. This option applies only to NetApp file servers.
- EVENTSERVER
  The EVENTSERVER option specifies whether at startup the server should try to contact the event server.
- EXPINTERVAL
  The EXPINTERVAL option specifies the interval, in hours, between automatic inventory expiration processes by IBM Spectrum Protect. Inventory expiration removes client backup and archive file copies from the server as specified by the management classes to which the client files are bound. If expiration is not run periodically, storage pool space is not reclaimed from expired client files, and the server requires more storage space than required by policy.
- EXPQUIET
  The EXPQUIET option specifies whether IBM Spectrum Protect sends detailed messages during expiration processing.
- Linux Windows FASPBEGPORT
  The FASPBEGPORT option specifies the starting number in the range of port numbers that are used for network communications with Aspera® Fast Adaptive Secure Protocol (FASP®) technology.
- Linux Windows FASPENDPORT
  The FASPENDPORT option specifies the ending number in the range of port numbers that are used for network communications with Aspera Fast Adaptive Secure Protocol (FASP) technology.

- Linux | Windows FASPTARGETRATE
  The FASPTARGETRATE option specifies the target rate for data transfer with Aspera Fast Adaptive Secure Protocol (FASP) technology. By specifying the target rate, you limit the bandwidth of each network connection that uses Aspera FASP technology. In this way, you can ensure that sufficient bandwidth is available for all network connections.
- FFDCLOGLEVEL
  The FFDCLOGLEVEL option specifies the type of general server messages that are displayed in the first failure data capture (FFDC) log.
- FFDCLOGNAME
  The FFDCLOGNAME option specifies a name for the first failure data capture (FFDC) log.
- FFDCMAXLOGSIZE
  The FFDCMAXLOGSIZE option specifies the size for the first failure data capture (FFDC) log file.
- FFDCNUMLOGS
  The FFDCNUMLOGS option specifies the number of log files that can be used for circular logging. The default value is 10.
- FILEEXIT
  The FILEEXIT option specifies a file to which enabled events are routed. Each logged event is a record in the file.
- FILETEXTEXIT
  The FILETEXTEXIT option specifies a file to which enabled events are routed. Each logged event is a fixed-size, readable line.
- FIPSMODE
  The FIPSMODE option specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for non-Secure Sockets Layer (SSL) operations.
- FSUSEDTHRESHOLD
  The FSUSEDTHRESHOLD option specifies what percentage of the file system can be filled up by the database before an alert message is issued.
- IDLETIMEOUT
  The IDLETIMEOUT option specifies the amount of time, in minutes, that a client session can be idle before the server cancels the session. You may want to increase the time-out value to prevent clients from timing out if there is a heavy network load in your environment. Note, however, that a large number of idle sessions could prevent other users from connecting to the server.
- KEEPALIVE
  The KEEPALIVE option specifies whether the Transmission Control Protocol (TCP) keepalive function is enabled for outbound TCP sockets. The TCP keepalive function sends a transmission from one device to another to check that the link between the two devices is operating.
- KEEPALIVETIME
  The KEEPALIVETIME option specifies how often TCP sends a keepalive transmission when it receives a response. This option applies only if you set the KEEPALIVE option to YES.
- KEEPALIVEINTERVAL
  The KEEPALIVEINTERVAL option specifies how often a keepalive transmission is sent if no response is received. This option applies only if you set the KEEPALIVE option to YES.
- LANGUAGE
  The LANGUAGE option controls the initialization of locales. A locale includes the language and the date, time, and number formats to be used for the console and server.
- LDAPCACHEDURATION
  The LDAPCACHEDURATION option determines the amount of time that the IBM Spectrum Protect server caches LDAP password authentication information.
- LDAPURL
  The LDAPURL option specifies the location of a Lightweight Directory Access Protocol (LDAP) server. Set the LDAPURL option after you configure the LDAP server.
- MAXSESSIONS
  The MAXSESSIONS option specifies the maximum number of simultaneous client sessions that can connect with the server.
- MESSAGEFORMAT
  The MESSAGEFORMAT option specifies whether a message number is displayed in all lines of a multi-line message.
- MIRRORLOGDIRECTORY
  The MIRRORLOGDIRECTORY option specifies the directory for mirroring the active log path.
- MOVEBATCHSIZE
  The MOVEBATCHSIZE option specifies the number of client files that are to be moved and grouped together in a batch, within the same server transaction. This data movement results from storage pool backups and restores, migration, reclamation, and MOVE DATA operations. This option works with the MOVESIZETHRESH option.
- MOVESIZETHRESH
  The MOVESIZETHRESH option specifies, in megabytes, a threshold for the amount of data moved as a batch, within the

same server transaction. When this threshold is reached, no more files are added to the current batch, and a new transaction is started after the current batch is moved.

- MSGINTERVAL
  The MSGINTERVAL option specifies the time, in minutes, between messages prompting an operator to mount a tape for the server.
- Windows NAMEDPIPENAME
  The NAMEDPIPENAME option specifies a communication method that allows processes to communicate with one another without having to know where the sender and receiver processes are located. The name acts like an alias, connecting the two processes regardless of whether they are on the same computer or across connected domains.
- NDMPCONNECTIONTIMEOUT
  The NDMPCONNECTIONTIMEOUT server option specifies the time in hours that IBM Spectrum Protect server waits to receive status updates during NDMP restore operations across the LAN. NDMP restore operations of large NAS file systems can have long periods of inactivity. The default is 6 hours.
- NDMPCONTROLPORT
  The NDMPCONTROLPORT option specifies the port number to be used for internal communications for certain Network Data Management Protocol (NDMP) operations. The IBM Spectrum Protect server does not function as a general purpose NDMP tape server.
- NDMPENABLEKEEPALIVE
  The NDMPENABLEKEEPALIVE server option specifies whether the IBM Spectrum Protect server enables Transmission Control Protocol (TCP) keepalive on network data-management protocol (NDMP) control connections to network-attached storage (NAS) devices. The default is NO.
- AIX Linux Windows NDMPKEEPIDLEMINUTES
  The NDMPKEEPIDLEMINUTES server option specifies the amount of time, in minutes, before the operating system transmits the first Transmission Control Protocol (TCP) keepalive packet on a network data-management protocol (NDMP) control connection. The default is 120 minutes.
- NDMPPORTRANGE
  The NDMPPORTRANGE option specifies the range of port numbers through which IBM Spectrum Protect cycles to obtain a port number for accepting a session from a network-attached storage (NAS) device for data transfer. The default is 0,0 which means that IBM Spectrum Protect lets the operating system provide a port (ephemeral port).
- NDMPPREFDATAINTERFACE
  This option specifies the IP address that is associated with the interface in which you want the server to receive all Network Data Management Protocol (NDMP) backup data.
- NOPREEMPT
  The server allows certain operations to preempt other operations for access to volumes and devices. You can specify the NOPREEMPT option to disable preemption. When preemption is disabled, no operation can preempt another for access to a volume, and only a database backup operation can preempt another operation for access to a device.
- NORETRIEVEDATE
  The NORETRIEVEDATE option specifies that the server does not update the retrieve date of a file in a disk storage pool when a client restores or retrieves the file. This option and the MIGDELAY storage pool parameter control when the server migrates files.
- Windows NPAUDITFAILURE
  The NPAUDITFAILURE option specifies whether an event is sent to the event log when a node logs in to the server using a name that is in the Windows group but does not match the Windows account login name. To ensure that a node can access only its own data, the node name and the Windows account name must match.
- Windows NPAUDITSUCCESS
  The NPAUDITSUCCESS option specifies that an event is sent to the event log when a client node user is authenticated for access to the server through SECUREPIPE.
- Windows NPBUFFERSIZE
  The NPBUFFERSIZE option specifies the size of the Named Pipes communication buffer.
- Windows NUMBERFORMAT
  The NUMBERFORMAT option specifies the format in which the server displays numbers.
- NUMOPENVOLSALLOWED
  The NUMOPENVOLSALLOWED option specifies the number of input FILE volumes in a deduplicated storage pool that can be open at one time.
- PUSHSTATUS
  The PUSHSTATUS option is used on spoke servers to ensure that status information is sent to the hub server. Do not update this option unless you must restore the Operations Center configuration to the preconfigured state where the IBM Spectrum Protect servers are not defined as hub or spoke servers.
- QUERYAUTH
  The QUERYAUTH option specifies the administrative authority level required to issue QUERY or SQL SELECT commands. By default any administrator can issue QUERY and SELECT commands. You can use this option to restrict the use of these commands.

- RECLAIMDELAY
  This option delays the reclamation of a SnapLock volume, allowing remaining data to expire so that there is no need to reclaim the volume.
- RECLAIMPERIOD
  This option allows you to set the number of days for the reclamation period of a SnapLock volume.
- REORGBEGINTIME
  The REORGBEGINTIME option specifies the earliest time that the IBM Spectrum Protect server can start a table or index reorganization.
- REORGDURATION
  The REORGDURATION option specifies an interval during which server-initiated table or index reorganization can start.
- REPORTRETRIEVE
  The REPORTRETRIEVE option reports on restore or retrieve operations that are performed by client nodes or administrators. The default is NO.
- REPLBATCHSIZE
  The REPLBATCHSIZE option specifies the number of client files that are to be replicated in a batch, within the same server transaction. This option affects only the node replication processes and works with the REPLSIZETHRESH option to improve node replication processing.
- REPLSIZETHRESH
  The REPLSIZETHRESH option specifies, in megabytes, a threshold for the amount of data replicated, within the same server transaction.
- REQSYSAUTHOUTFILE
  The REQSYSAUTHOUTFILE option specifies if system authority is required for administrative commands that cause IBM Spectrum Protect to write to an external file.
- RESOURCETIMEOUT
  The RESOURCETIMEOUT option specifies how long the server waits for a resource before canceling the pending acquisition of a resource. When a timeout occurs the request for the resource will be canceled.
- RESTHTTPSPORT
  The RESTHTTPSPORT option specifies the port number to be used for Hypertext Transfer Protocol Secure (HTTPS) communication between the Operations Center and the hub server.
- RESTOREINTERVAL
  The RESTOREINTERVAL option specifies how long a restartable restore session can be saved in the server database. As long as the restore session is saved in the database, it can be restarted from the point at which it stopped.
- RETENTIONEXTENSION
  The RETENTIONEXTENSION option specifies the number of days to extend the retention date of a SnapLock volume. This option allows the server to extend the retention date of a SnapLock volume in order to avoid excessive reclamation.
- AIX Linux Windows SANDISCOVERY
  The SANDISCOVERY option specifies whether the IBM Spectrum Protect SAN discovery function is enabled.
- AIX Linux Windows SANDISCOVERYTIMEOUT
  The SANDISCOVERYTIMEOUT option specifies the amount of time allowed for host bus adapters to respond when they are queried by the SAN discovery process. Once the time specified for the SANDISCOVERYTIMEOUT is reached, the process times out.
- AIX Linux Windows SANREFRESHTIME
  The SANREFRESHTIME option specifies the amount of time that elapses before the cached SAN discovery information is refreshed. The SANREFRESHTIME option has a default value of 0, which means that there is no SAN discovery cache. The information is obtained directly from the host bus adapter (HBA) every time the server performs a SAN discovery operation.
- SEARCHMPQUEUE
  The SEARCHMPQUEUE option specifies the order in which the server satisfies requests in the mount queue. If the option is specified, the server first tries to satisfy requests for volumes that are already mounted. These requests may be satisfied before other requests, even if the others have been waiting longer for the mount point. If this option is not specified, the server satisfies requests in the order in which they are received.
- Windows SECUREPIPES
  When using the named pipes protocol, enabling SECUREPIPES forces the server to check the Windows group designated by ADSMGROUPNAME in order to authenticate a client node/user.
- SERVERDEDUPTXNLIMIT
  The SERVERDEDUPTXNLIMIT option specifies the maximum size of objects that can be deduplicated on the server.
- SHMPORT
  AIX Linux The SHMPORT option specifies the TCP/IP port address of a server when using shared memory. All shared memory communications start with a TCP/IP connection. Windows The SHMPORT option specifies the port that the server listens on for shared memory connections.
- SHREDDING
  The SHREDDING option specifies whether shredding of deleted sensitive data is performed automatically or manually. Shredding applies only to data in storage pools that have been explicitly configured to support shredding.

- SNMPHEARTBEATINTERVAL
  The SNMPHEARTBEATINTERVAL option specifies the interval in minutes between queries of the IBM Spectrum Protect server.
- SNMPMESSAGECATEGORY
  The SNMPMESSAGECATEGORY option specifies the trap types used when messages are forwarded from the server, through the Simple Network Management Protocol (SNMP) subagent, to the SNMP manager.
- SNMPSUBAGENT
  The SNMPSUBAGENT option specifies the parameters needed for the IBM Spectrum Protect subagent to communicate with the Simple Network Management Protocol (SNMP) daemon. This option is only to configure the SNMP subagent for communicating with the SNMP agent; it is ignored by the server.
- SNMPSUBAGENTHOST
  The SNMPSUBAGENTHOST option specifies the location of the IBM Spectrum Protect Simple Network Management Protocol (SNMP) subagent. The default for this option is 127.0.0.1.
- SNMPSUBAGENTPORT
  The SNMPSUBAGENTPORT option specifies the port number of the IBM Spectrum Protect Simple Network Management Protocol (SNMP) subagent.
- SSLFIPSMODE
  The SSLFIPSMODE option specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for Secure Sockets Layer (SSL). The default is NO.
- SSLINITTIMEOUT
  The SSLINITTIMEOUT option specifies the time, in minutes, that the server waits for a Secure Sockets Layer (SSL) session to complete initialization before the server cancels the session.
- SSLTCPADMINPORT
  The SSLTCPADMINPORT option specifies the port address on which the server TCP/IP communication driver waits for requests for SSL-enabled sessions only. The sessions are for the command-line administrative client.
- SSLTCPPORT
  The SSLTCPPORT option specifies the Secure Sockets Layer (SSL) port number for SSL-enabled sessions only. The server TCP/IP communication driver waits for requests on this port for SSL-enabled sessions from the client.
- TCPADMINPORT
  The TCPADMINPORT option specifies the port number on which the server TCP/IP communication driver waits for requests for TCP/IP and SSL-enabled sessions other than client sessions. This includes administrative sessions, server-to-server sessions, storage agent sessions, library client sessions, managed server sessions, and event server sessions.
- AIX Linux TCPBUFSIZE
  The TCPBUFSIZE option specifies the size of the buffer used for TCP/IP send requests. During a restore, client data moves from the IBM Spectrum Protect session component to a TCP communication driver. The TCPBUFSIZE option determines if the server sends the data directly from the session buffer or copies the data to the TCP buffer. A 32 KB buffer size forces the server to copy data to its communication buffer and flush the buffer when it fills.
- TCPNODELAY
  The TCPNODELAY option specifies whether the server disables the delay of sending successive small packets on the network.
- TCPPORT
  The TCPPORT option specifies the port number on which the server TCP/IP communication driver waits for requests for client sessions. The server TCP/IP communication driver listens on this port for both TCP/IP and SSL-enabled sessions from the client.
- TCPWINDOWSIZE
  The TCPWINDOWSIZE option specifies, in kilobytes, the amount of receive data that can be buffered at one time on a TCP/IP connection. The sending host cannot send more data until it receives an acknowledgment and a TCP receive window update. Each TCP packet contains the advertised TCP receive window on the connection. A larger window lets the sender continue sending data, and may improve communication performance, especially on fast networks with high latency.
- TECBEGINEVENTLOGGING
  The TECBEGINEVENTLOGGING option specifies whether event logging for the Tivoli® receiver should begin when the server starts up. If the TECHOST option is specified, TECBEGINEVENTLOGGING defaults to YES.
- TECHOST
  The TECHOST option specifies the host name or IP address for the Tivoli event server.
- TECPORT
  The TECPORT option specifies the TCP/IP port address on which the Tivoli event server is listening. This option is only required if the Tivoli event server is on a system that does not have a Port Mapper service running.
- TECUTF8EVENT
  The TECUTF8EVENT option allows the IBM Spectrum Protect administrator to send information to the Tivoli Enterprise Console® (TEC) server in UTF–8 data format. The default is No. You can display whether or not this option is enabled by issuing the QUERY OPTION command.

- THROUGHPUTDATATHRESHOLD
  The THROUGHPUTDATATHRESHOLD option specifies a throughput threshold that a client session must reach to prevent being canceled after the time threshold is reached.
- THROUGHPUTTIMETHRESHOLD
  The THROUGHPUTTIMETHRESHOLD option specifies the time threshold for a session after which it may be canceled for low throughput.
- Windows TIMEFORMAT
  The TIMEFORMAT option specifies the format in which time is displayed by the server.
- TXNGROUPMAX
  The TXNGROUPMAX option specifies the number of objects that are transferred as a group between a client and the server between transaction commit points. The minimum value is 4 objects and the maximum value is 65000 objects. The default value is 4096 objects. The objects transferred are actual files, directories, or both. The server counts each file or directory as one object.
- UNIQUETDPTECEVENTS
  The UNIQUETDPTECEVENTS option generates a unique Tivoli Enterprise Console (TEC) event class for each individual IBM Spectrum Protect message, including client, server, and IBM Spectrum Protect Data Protection client messages. The default is No.
- UNIQUETECEVENTS
  The UNIQUETECEVENTS option generates a unique Tivoli Enterprise Console (TEC) event class for each individual IBM Spectrum Protect message. The default is No.
- USEREXIT
  The USEREXIT option specifies a user-defined exit that will be given control to manage an event.
- VERBCHECK
  The VERBCHECK option specifies that the server will do additional error checking on the structure of commands sent by the client. This option should only be enabled when the client sends incorrectly formed requests to the server, causing the server to crash. When this option is enabled, you will get a protocol error instead of a server crash.
- VOLUMEHISTORY
  The VOLUMEHISTORY option specifies the name of files to be automatically updated whenever server sequential volume history information is changed. There is no default for this option.

Modifying server options

The server reads the server options file at server initialization. When you update a server option by editing the file, you must stop and start the server to activate the updated server options file.

About this task

You can change some options dynamically without stopping and starting the server, by using the SETOPT command. See SETOPT (Set a server option for dynamic update) for details.

AIX Linux The dsmserv.opt.smp file (also provided at installation) contains the format of the options file and all the default settings. You can change any options in the dsmserv.opt.smp file. To have the server use the changed options, you must rename the file to dsmserv.opt. To activate an option within the server options file, remove the *>>> that precedes the option. The server ignores any options preceded by *>>>.

Windows You can modify server options by using the options file editor included in the IBM Spectrum Protect™ Console. This editor provides communications parameter detection, value validation, and help for all options. The options file editor is the preferred way to change server options, but you can also use a text editor.

Types of server options

Server options let you customize how some functions and processes work.

- Server communication options
  You can use server options to specify server communication methods and their characteristics.
- Server storage options
  IBM Spectrum Protect provides a number of options that you can specify to configure certain device and server storage operations.
- Client-server options
  You can use server options to control client-server processing.

- Date, number, time, and language options
  You can use server options to specify display formats for the dates, times, numbers, and national language.
- Database options
  You can use server options to control some aspects of database processing.
- Data transfer options
  You can use server options to control how IBM Spectrum Protect groups and transfers data.
- Message options
  You can use server options to give you more flexibility in the way IBM Spectrum Protect issues messages.
- Event logging options
  Options can help you manage event logging receivers.
- Security options and licensing options
  You can use server options to customize server security and license audits.
- Miscellaneous options
  You can use a variety of miscellaneous server options to customize IBM Spectrum Protect.

Server communication options

You can use server options to specify server communication methods and their characteristics.

Table 1. Communication options

Option	Description
ADMINCOMMTIMEOUT	The amount of time that the server waits for an administrative client message during an operation that causes a database update
ADMINIDLETIMEOUT	The amount of time an administrative client session can be idle
ADMINONCLIENTPORT	The port that determines whether administrative sessions can use the port specified in the TCPPORT option
COMMMETHOD	The server communication method
DBMTCPPORT	The port number on which the TCP/IP communication driver for the database manager waits for client session requests
DNSLOOKUP	Control of use of Domain Name Services to lookup names of systems contacting the server
FIPSMODE	Specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for non-SSL operations.
LDAPCACHEDURATION	Determines the amount of time that authentication sessions, to the same node or administrator, are skipped. You might see a slight performance boost when skipping sessions.
LDAPURL	Specifies the LDAP directory server. Each setting must have the LDAP directory server name, a port number, and the base distinguished name of the namespace or suffix that the server maintains.
Windows NAMEDPIPENAME	Windows The named pipes communication method
NDMPCONTROLPORT	The internal communications port used for certain Network Data Management Protocol (NDMP) operations

Option	Description
NDMPENABLEKEEPALIVE	The TCP keepalive mechanism
AIX Linux Windows NDMPKEEPIDLEMINUTES	AIX Linux Windows The amount of idle time before the first TCP keepalive packet is sent
Windows NPBUFFERSIZE	Windows The size of the Named Pipes communication buffer
SHMPORT	AIX Linux The TCP/IP port address of a server when using shared memory Windows The port that the server listens on for shared memory connections
SNMPHEARTBEATINTERVAL	The interval in minutes between queries of the IBM Spectrum Protect server
SNMPMESSAGECATEGORY	The trap types used when messages are forwarded from the server
SNMPSUBAGENT	The parameters needed for the IBM Spectrum Protect subagent to communicate with the SNMP daemon
SNMPSUBAGENTHOST	The location of the IBM Spectrum Protect SNMP subagent
SNMPSUBAGENTPORT	The port address of the IBM Spectrum Protect SNMP subagent
SSLFIPSMODE	Specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for Secure Sockets Layer (SSL)
SSLTCPADMINPORT	The port address on which the server's TCP/IP communication driver waits for requests for SSL-enabled sessions for the command-line administrative client
SSLTCPPORT	The SSL-only port number on which the server's TCP/IP communication driver waits for requests for SSL-enabled sessions from the following sources: • Command line backup-archive client • Backup-archive GUI • Administrative client • Application programming interface (API)
TCPADMINPORT	The TCP/IP port number for administrative sessions
AIX Linux TCPBUFSIZE	AIX Linux The size of the buffer used for TCP/IP send requests
TCPPORT	The TCP/IP port number for client sessions
TCPWINDOWSIZE	The client node TCP/IP sliding window

Server storage options

IBM Spectrum Protect™ provides a number of options that you can specify to configure certain device and server storage operations.

Table 1. Server storage options

Option	Description
3494SHARED	Enables sharing of a 3494 library with applications other than IBM Spectrum Protect.
ACSACCESSID	The ID for the ACS access control.
ACSLOCKDRIVE	Allows the drives within the ACSLS libraries to be locked.
ACSQUICKINIT	Allows a quick or full initialization of the ACSLS library.
ACSTIMEOUTX	The multiple for the built-in timeout value for the ACSLS API.
ASSISTVCRRECOVERY	Specifies whether the server assists an IBM 3590 drive in recovering from a lost or corrupted Vital Cartridge Records (VCR) condition.
CHECKTAPEPOS	Specifies whether the server validates data position on tape.
CLIENTDEDUPTXNLIMIT	Specifies the maximum size of a transaction when client-side deduplicated data is backed up or archived.
DEDUPREQUIRESBACKUP	Specifies whether volumes in primary sequential-access storage pools that are set up for data deduplication can be reclaimed and whether duplicate data can be discarded before the storage pools are backed up.
DEDUPTIER2FILESIZE	File size at which Tier 2 processing is used for data deduplication.
DEDUPTIER3FILESIZE	File size at which Tier 3 processing is used for data deduplication.
DEVCONFIG	The name of the file that store backup copies of device configuration information.
DRIVEACQUIRERETRY	The number of times that the server retries the acquisition of a drive in an IBM 349x library that is shared among multiple applications.
ENABLENASDEDUP	Specifies whether the server deduplicates data that is stored by a NetApp network-attached storage (NAS) file server.
NUMOPENVOLSALLOWED	The number of input FILE volumes in a deduplicated storage pool that can be open at one time.
RECLAIMDELAY	The number of days that the reclamation of a SnapLock volume is delayed.
RECLAIMPERIOD	The number of days for the reclamation period of a SnapLock volume
RESOURCETIMEOUT	The length of time that the server waits for a resource before canceling the pending acquisition of the resource.
RETENTIONEXTENSION	The number of days to extend the retention date of a SnapLock volume.
AIX Linux Windows SANDISCOVERY	AIX Linux Windows Whether the IBM Spectrum Protect SAN discovery function is enabled.
AIX Linux Windows SANDISCOVERYTIMEOUT	AIX Linux Windows Amount of time before the SAN discovery process times out.
AIX Linux Windows SANREFRESHTIME	AIX Linux Windows Amount of time before cached SAN discovery information is refreshed.
SEARCHMPQUEUE	The order in which the server satisfies requests in the mount queue.
SERVERDEDUPTXNLIMIT	Specifies the maximum size of objects that can be deduplicated on the server.

Client-server options

You can use server options to control client-server processing.

Table 1. Client-Server options

Option	Description

Option	Description
COMMTIMEOUT	The number of seconds the server waits for a response from a client before timing out the client session
DISABLESCHEDS	Whether administrative and client schedules are disabled during the IBM Spectrum Protect server recovery scenario
IDLETIMEOUT	The number of minutes the server allows a client session to remain idle before timing out the client session
MAXSESSIONS	The maximum number of simultaneous client sessions with the server
THROUGHPUTDATATHRESHOLD	The throughput threshold that a client session must reach to prevent being canceled after the time threshold is reached
THROUGHPUTTIMETHRESHOLD	The time threshold for a session after which it may be canceled for low throughput
VERBCHECK	Whether additional error checking is done for commands sent by the client

Date, number, time, and language options

You can use server options to specify display formats for the dates, times, numbers, and national language.

Table 1. Date, number, time, and language options

Option	Description
Windows DATEFORMAT	Windows The format by which dates are displayed
LANGUAGE	The national language is used to present client messages
Windows NUMBERFORMAT	Windows The format for displaying numbers
Windows TIMEFORMAT	Windows The format displaying times

Database options

You can use server options to control some aspects of database processing.

Table 1. Database options

Option	Description
ACTIVELOGDIRECTORY	The new directory for the location where the active log is stored. Use this option to change the location of the active log.
ACTIVELOGSIZE	The maximum size of the active log.
ALLOWREORGINDEX	Server-initiated index reorganization.
ALLOWREORGTABLE	Server-initiated table reorganization.
ARCHLOGDIRECTORY	The directory that the database manager can archive a log file into after all the transactions represented in that log file are completed.
ARCHFAILOVERLOGDIRECTORY	The directory in which the server tries to store archive log files that cannot be stored in the archive log directory.
DBDIAGLOGSIZE	The maximum size of the database manager diagnostic log files.
DBDIAGPATHFSTHRESHOLD	The threshold for free space on the file system or disk that contains the database manager diagnostic log files.
DBMEMPERCENT	The percentage of system memory that is dedicated to the database.
DISABLEREORGTABLE	Disables table reorganization for specific tables.
FSUSEDTHRESHOLD	The percentage of the file system that can be used by the database before an alert message is issued.
MIRRORLOGDIRECTORY	The directory for mirroring the active log path.

Option	Description
REORGBEGINTIME	The earliest time that the IBM Spectrum Protect server can start a table or index reorganization.
REORGDURATION	The interval during which server-initiated table or index reorganization can start.

Data transfer options

You can use server options to control how IBM Spectrum Protect™ groups and transfers data.

Table 1. Group options

Option	Description
MOVEBATCHSIZE	The number of files that are to be moved and grouped in a batch, within a transaction
MOVESIZETHRESH	The threshold for the amount of data moved as a batch, within the same server transaction
NDMPPORTRANGE	The IP address associated with the interface in which the server receives all Network Data Management Protocol (NDMP) backup data
NDMPPREFDATAINTERFACE	The IP address associated with the interface in which the server receives all Network Data Management Protocol (NDMP) backup data
REPLBATCHSIZE	The number of files that are to be replicated in a batch, within the same server transaction
REPLSIZETHRESH	The threshold for the amount of data replicated as a batch, within the same server transaction
TXNGROUPMAX	The number of files that are transferred as a group between a client and the server between transaction commit points

Message options

You can use server options to give you more flexibility in the way IBM Spectrum Protect™ issues messages.

Table 1. Message options

Option	Description
EXPQUIET	Whether IBM Spectrum Protect sends detailed informational messages during expiration processing
MESSAGEFORMAT	Whether a message number is displayed in all lines of a multi-line message
MSGINTERVAL	The time, in minutes, between messages prompting an operator to mount a tape for IBM Spectrum Protect

Event logging options

Options can help you manage event logging receivers.

Table 1. Event logging options

Option	Description
EVENTSERVER	Whether the server should try to contact the event server when the server starts up
FILEEXIT	A file to which enabled events are routed (binary format)
FILETEXTEXIT	A file to which enabled events are routed (readable format)
REPORTRETRIEVE	Record client restore and retrieve operations
TECBEGINEVENTLOGGING	Whether event logging for the TIVOLI receiver should begin when the server starts up

Option	Description
TECHOST	The host name or IP address for the Tivoli Enterprise Console (TEC) event server
TECPORT	The TCP/IP port address on which the Tivoli Enterprise Console event server is listening
TECUTF8EVENT	A Tivoli Enterprise Console event sent from the IBM Spectrum Protect server in UTF8 format
UNIQUETDPTECEVENTS	Events from an IBM Spectrum Protect Data Protection client that are sent to the Tivoli Enterprise Console as unique events
UNIQUETECEVENTS	Events sent to the Tivoli Enterprise Console as unique
USEREXIT	A user-defined exit that will be given control to manage an event

Security options and licensing options

You can use server options to customize server security and license audits.

Table 1. Security and licensing options

Option	Description
Windows ADSMGROUPNAME	Windows The name of a Windows group
AUDITSTORAGE	Specifies that during a license audit operation, the server calculates, by node, the amount of backup, archive, and space management storage in use
BACKUPINITIATIONROOT	Specifies whether the server overrides node parameter values for users who are not IBM Spectrum Protect authorized users
LDAPURL	Specifies the LDAP directory server. Each setting must have the LDAP directory server name, a port number, and the base distinguished name of the namespace or suffix that the server maintains.
Windows NPAUDITFAILURE	Windows Specifies that a node can access only its own data
Windows NPAUDITSUCCESS	Windows Specifies that an event is sent to the event log when a client node user is authenticated for access to the server through SECUREPIPE
QUERYAUTH	The administrative authority level required to issue QUERY or SQL SELECT commands
REQSYSAUTHOUTFILE	Specifies if system authority is required for administrative commands that cause IBM Spectrum Protect to write to an external file
Windows SECUREPIPES	Windows With named pipes protocol, specifies that the server checks the Windows group to authenticate a client
SHREDDING	Specifies whether shredding of deleted sensitive data is done automatically or manually

Related reference:
Server communication options

Miscellaneous options

You can use a variety of miscellaneous server options to customize IBM Spectrum Protect™.

Table 1. Miscellaneous options

Option	Description
ALIASHALT	Allows administrators to give the IBM Spectrum Protect HALT command a different name

Option	Description
DISPLAYLFINFO	Specifies whether accounting records and summary table entries report the storage agent name
EXPINTERVAL	The interval between automatic inventory expiration processes
FFDCLOGNAME	The name for the first failure data capture (FFDC) log
FFDCMAXLOGSIZE	The maximum size of the first failure data capture (FFDC) log
NOPREEMPT	Specifies that no operation can preempt another for access to a volume and that only a database backup operation can preempt another operation for access to a device
NORETRIEVEDATE	Specifies that the server does not update the retrieve date of a file in a disk storage pool when a client restores or retrieves the file
RESTOREINTERVAL	The length of time that a restartable restore session can be saved in the server database
VOLUMEHISTORY	The name of the file to be automatically updated whenever server sequential volume history information is changed

3494SHARED

The 3494SHARED option specifies whether an IBM® 3494 library can share applications other than IBM Spectrum Protect™.

The default is NO, meaning that no application other than IBM Spectrum Protect can share the 3494. When you set this option to YES, for every mount request, IBM Spectrum Protect determines if each drive is in use. After the query completes, IBM Spectrum Protect selects an available drive that is not in use by another application. Enable sharing only if you have more than two drives in your library. If you are currently sharing an IBM 3494 library with other applications, you must specify this option.

Syntax

```
>>-3494SHARED--+-Yes-+-----------------------------------------><
               '-No--'
```

Parameters

Yes
: Specifies that other applications can share the 3494 library.

No
: Specifies that no other applications can share the 3494 library.

Examples

Enable sharing of a 3494 library:

```
3494shared yes
```

ACSACCESSID

The ACSACCESSID option specifies the ID for the ACS access control for an ACSLS library.

Syntax

```
>>-ACSACCESSID--name-------------------------------------------><
```

Parameters

name
: Specifies a 1 to 64 character ID. The default ID is your local host name.

Examples

```
acsaccessid region
```

ACSLOCKDRIVE

The ACSLOCKDRIVE option specifies if the drives within the ACSLS libraries are locked. Drive locking ensures the exclusive use of the drive in the ACSLS library in a shared environment. However, there is some performance gain if libraries are not locked. When other applications do not share the IBM Spectrum Protect™ drives, drive locking is not required.

Syntax

```
>>-ACSLOCKDRIVE--+-Yes-+---------------------------------------><
                 '-No--'
```

Parameters

Yes
: Specifies that drives are locked.

No
: Specifies that drives are not locked.

Examples

```
acslockdrive yes
```

ACSQUICKINIT

The ACSQUICKINIT option specifies whether, at server startup, the initialization of the ACSLS library is a quick or full initialization. The default is Yes. A quick initialization avoids the overhead associated with synchronizing the IBM Spectrum Protect™ server inventory with the ACSLS library inventory (through an audit of the library).

Syntax

```
>>-ACSQUICKINIT--+-Yes-+---------------------------------------><
                 '-No--'
```

Parameters

Yes

: Specifies that a quick initialization of the ACSLS library is performed. When the option is set to Yes, IBM Spectrum Protect bypasses library inventory verification, initializing the library quickly, and making it available to IBM Spectrum Protect sooner than if a full initialization is done.

This option should be set to Yes when it is known that the physical library inventory and the IBM Spectrum Protect library inventory have not changed and an audit is not needed.

No

Specifies that a full initialization of the ACSLS library and library inventory is performed. When the option is set to No, IBM Spectrum Protect synchronizes its library volume inventory with what is reported by the ACSLS library manager.

Examples

```
acsquickinit yes
```

ACSTIMEOUTX

The ACSTIMEOUTX option specifies the multiple for the built-in timeout value for ACSLS APIs. The built-in timeout value for the ENTER, EJECT, and AUDIT ACS API is 1800 seconds; for all other ACSLS APIs it is 600 seconds. For example, if the multiple value specified is 5, the timeout value for audit API becomes 9000 seconds, and all other APIs become 3000 seconds.

Syntax

```
>>-ACSTIMEOUTX--value-----------------------------------------><
```

Parameters

value
Specifies the multiple for the built-in timeout value for ACSLS API. The range is from 1 to 100. The default is 1.

Examples

```
acstimeoutx 1
```

ACTIVELOGDIRECTORY

The ACTIVELOGDIRECTORY option specifies the name of the directory where all active logs are stored.

This option is appended to the options file when the DSMSERV FORMAT command is run. Under normal operating conditions, the option does not need to be changed. See DSMSERV FORMAT (Format the database and log) for guidance on this option.

Syntax

```
>>-ACTIVELOGDirectory--dir_name-------------------------------><
```

Parameters

dir_name
Specifies a fully qualified directory name. The directory must exist, it must be empty, and it must be accessible by the user ID of the database manager. If you change the active log directory, IBM Spectrum Protect™ moves the existing active logs to the location that is specified by this directory. The maximum number of characters is 175.

Examples

AIX | Linux

```
activelogdirectory /tsm/activelogdir
```

Windows

```
activelogdirectory c:\tsmserv1\activelogdir
```

ACTIVELOGSIZE

The ACTIVELOGSIZE option sets the total log size.

This option is appended to the options file when the DSMSERV FORMAT command is run. Under normal operating conditions the option does not need to be changed. See DSMSERV FORMAT (Format the database and log) for guidance on this option.

Syntax

```
                    .-16GB------.
>>-ACTIVELOGSize--+-megabytes-+--------------------------------><
```

Parameters

megabytes
: Specifies the size of the active log file in megabytes. The minimum value is 2048 MB (2 GB); the maximum is 524,288 MB (512 GB). If an odd number is specified, the value is rounded up to the next even number. The default is 16,384 MB (16 GB).
The size of an active log file is based on the value of the ACTIVELOGSIZE option. Guidelines for space requirements are in the following table:

Table 1. How to estimate volume and file space requirements

ACTIVELOGSize option value	Reserve this much free space in the active log directory, in addition to the ACTIVELOGSize space
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Examples

```
activelogsize 8192
```

ADMINCOMMTIMEOUT

The ADMINCOMMTIMEOUT option specifies how long the server waits for an expected administrative client message during an operation that causes a database update.

If the length of time exceeds this time-out period, the server ends the session with the administrative client. You may want to increase the time-out value to prevent administrative client sessions from timing out.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
                      .-60------.
>>-ADMINCOMMTimeout--+-seconds-+--------------------------------><
```

Parameters

seconds
: Specifies the maximum number of seconds that a server waits for an administrative client response. The default value is 60. The minimum value is 1.

Examples

```
admincommtimeout 60
```

ADMINIDLETIMEOUT

The ADMINIDLETIMEOUT option specifies the amount of time, in minutes, that an administrative client session can be idle before the server cancels the session.

If there is a heavy network load in your environment, you might want to increase the time-out value to prevent administrative clients from timing out. However, a large number of idle sessions could prevent other users from connecting to the server.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
                    .-15------.
>>-ADMINIDLETIMEOUT--+-minutes-+------------------------------><
```

Parameters

minutes
: Specifies the maximum number of minutes that a server waits for an idle administrative client. The default value is 15 minutes. The minimum value is 1 minute.

Examples

```
adminidletimeout 20
```

ADMINONCLIENTPORT

The ADMINONCLIENTPORT option specifies whether the TCPPORT can be used by administrative sessions. The default is YES.

Syntax

```
>>-ADMINONCLIENTPORT--+-YES-+-----------------------------------><
                      '-NO--'
```

Parameters

YES
: If the option is set to YES, or if the TCPPORT and TCPADMINPORT are the same value (the default), administrative sessions can use the TCPPORT.

NO
: If the option is set to NO, and if the TCPADMINPORT value is different than the TCPPORT value, administrative sessions cannot use the TCPPORT.

Examples

Specify that the TCPPORT can be used by administrative sessions.

```
adminonclientport yes
```

Windows

ADSMGROUPNAME

The ADSMGROUPNAME option specifies the name of a Windows group. A client node must be a member of this group to use the IBM Spectrum Protect™ server through NT Unified Logon. The client node must also be a registered IBM Spectrum Protect client node.

Syntax

```
>>-ADSMGROUPname--group_name-----------------------------------><
```

Parameters

group_name
: Specifies a Windows group name.

Examples

Specify IDD as a Windows group:

```
adsmgroup idd
```

ALIASHALT

The ALIASHALT option allows administrators to give the IBM Spectrum Protect™ **HALT** command a different name.

The administrative client recognizes an alias for the HALT command when the client is started with the CHECKALIASHALT option specified. See Administrative client options for details.

Syntax

```
>>-ALIASHALT--newname---------------------------------------><
```

Parameters

newname
: Specifies the alias of the HALT command for shutting down the IBM Spectrum Protect server. Minimum length of *newname* is 1; maximum length is 16.

Examples

```
aliashalt tsmhalt
```

ALLOWDESAUTH

The ALLOWDESAUTH option specifies whether to allow use of the Data Encryption Standard (DES) algorithm for authentication between a server and a backup-archive client.

To prevent the use of DES, specify a value of NO for the ALLOWDESAUTH option.
To configure the IBM Spectrum Protect™ server to be in compliance with the NIST SP800-131A standard, set this option to NO.
Restrictions:

- The backup-archive client must be running Version 6.3 or later if you authenticate to a server with the ALLOWDESAUTH option set to NO.
- Automatic deployment of the backup-archive client fails if this option is set to NO.

Syntax

```
   .-ALLOWDESAUTH--Yes-----.
>>-+----------------------+-----------------------------------><
   '-ALLOWDESAUTH--+-No--+-'
                   '-Yes-'
```

Parameters

Yes
: Specifies that the server allows authentication with any backup-archive clients that use DES-based encryption. The default is YES.

No
: Specifies that the server rejects any backup-archive clients that attempt to authenticate with DES-based encryption.

Examples

Specify that the server rejects any backup-archive clients that attempt to authenticate with DES encryption:

```
allowdesauth no
```

Specify that the server allows authentication with any backup-archive clients that use DES encryption:

```
allowdesauth yes
```

ALLOWREORGINDEX

The ALLOWREORGINDEX option specifies whether server-initiated index reorganization is enabled or disabled.

The default is YES.

Syntax

```
>>-ALLOWREORGINDEX--+-Yes-+-----------------------------------><
                    '-No--'
```

Parameters

Yes
: Specifies that server-initiated index reorganization is enabled.

No
: Specifies that server-initiated index reorganization is disabled.

Example

Specify that server-initiated index reorganization is enabled.

```
allowreorgindex yes
```

ALLOWREORGTABLE

The ALLOWREORGTABLE option specifies whether server-initiated table reorganization is enabled or disabled.

The default is YES.

Syntax

```
>>-ALLOWREORGTABLE--+-Yes-+-----------------------------------><
                    '-No--'
```

Parameters

Yes
: Specifies that server-initiated table reorganization is enabled.

No
: Specifies that server-initiated table reorganization is disabled.

Examples

Specify that server-initiated table reorganization is disabled.

```
allowreorgtable no
```

ARCHFAILOVERLOGDIRECTORY

The ARCHFAILOVERLOGDIRECTORY option specifies the directory which the server uses to store archive log files that cannot be stored in the archive log directory.

This option is appended to the options file when the DSMSERV FORMAT command is run. Typically the directory does not need to be changed.

Syntax

```
>>-ARCHFailoverlogdirectory--dir_name--------------------------><
```

Parameters

dir_name
: Specifies a fully qualified directory name. The maximum number of characters is 175.

Examples

AIX | Linux

```
archfailoverlogdirectory /tsm/archfailoverlog
```

Windows

```
archfailoverlogdirectory c:\tsmserv1\archfailoverlog
```

ARCHLOGCOMPRESS

You can enable or disable compression of archive logs on the IBM Spectrum Protect™ server. By compressing the archive logs, you reduce the amount of space that is required for storage.

The ARCHLOGCOMPRESS server option specifies whether log files that are written to the archive directory for logs are compressed.

Syntax

```
                    .-No--.
>>-ARCHLOGCOMPress--+-----+-----------------------------------><
                    '-Yes-'
```

Parameters

No
: Specifies that log files that are written to the archive log directory are not compressed. The default is No.

Yes
: Specifies that log files that are written to the archive log directory are compressed.

Restriction: Use caution when you enable the ARCHLOGCOMPRESS server option on systems with sustained high volume usage and heavy workloads. Enabling this option in this system environment can cause delays in archiving log files from the active log file system to the archive log file system. This delay can cause the active log file system to run out of space. Be sure to monitor the available space in the active log file system after archive log compression is enabled. If the active log directory file system usage nears out of space conditions, the ARCHLOGCOMPRESS server option must be disabled. You can use the SETOPT command to disable archive log compression immediately without halting the server.

Example

To enable compression of log files that are written to the archive log directory, specify the following option:

```
archlogcompress yes
```

ARCHLOGDIRECTORY

The ARCHLOGDIRECTORY option specifies a directory that the database manager can archive a log file into after all the transactions represented in that log file are completed.

This option is appended to the options file when the DSMSERV FORMAT command is run.

Syntax

```
>>-ARCHLOGDirectory--dir_name---------------------------------><
```

Parameters

dir_name
: Specifies a fully qualified directory name. The maximum number of characters is 175.

Examples

AIX | Linux

```
archlogdirectory /tsm/archlog
```

Windows

```
archlogdirectory d:\tsmserv1\archlog
```

ARCHLOGUSEDTHRESHOLD

The ARCHLOGUSEDTHRESHOLD option specifies when to start an automatic database backup in relation to the percentage of archive log file space used. The default is 80 percent.

The ARCHLOGUSEDTHRESHOLD option prevents frequent automatic backups. For example, if the archive log file directory resides on a file system or drive that is 400 GB, a database backup is triggered if there is less than 80 GB of free space. Repeated database backups might cause the server to use an excessive amount of scratch tapes.

Syntax

```
                          .-80----.
>>-ARCHLOGUSEDTHRESHOLD--+-value-+-----------------------------><
```

Parameters

value
: The percentage of archive log file space used before an automatic backup starts.

Specify to start an automatic backup when 90 percent of archive log file space is used.

```
archlogusedthreshold 90
```

ASSISTVCRRECOVERY

The ASSISTVCRRECOVERY option specifies whether IBM Spectrum Protect™ assists an IBM® 3590 drive in recovering from a lost or corrupted Vital Cartridge Records (VCR) condition. If you specify YES (the default) and if IBM Spectrum Protect detects an error

during the mount processing, it locates to the end-of-data during the dismount processing to allow the drives to restore the VCR. During the tape operation, there might be some small effect on performance because the drive cannot complete a fast locate with a lost or corrupted VCR. However, there is no loss of data.

Syntax

```
>>-ASSISTVCRRECovery--+-Yes-+---------------------------------><
                     '-No--'
```

Parameters

Yes
: Specifies server assistance in recovery.

No
: Specifies no server assistance in recovery.

Examples

Turn off recovery assistance:

```
assistvcrrecovery no
```

AUDITSTORAGE

As part of a license audit operation, the server calculates, by node, the amount of server storage used for backup, archive, and space–managed files. For servers managing large amounts of data, this calculation can take a great deal of CPU time and can stall other server activity. You can use the AUDITSTORAGE option to specify that storage is not to be calculated as part of a license audit.

Note: This option was previously called NOAUDITSTORAGE.

Syntax

```
>>-AUDITSTorage--+-Yes-+---------------------------------------><
                 '-No--'
```

Parameters

Yes
: Specifies that storage is to be calculated as part of a license audit. The default is Yes.

No
: Specifies that storage is not to be calculated as part of a license audit.

Examples

```
auditstorage    yes
```

BACKUPINITIATIONROOT

The BACKUPINITIATIONROOT option specifies whether the server overrides node parameter values for users who are not IBM Spectrum Protect™ authorized users.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-BACKUPINITIATIONROOT--+-ON--+------------------------------><
                        '-OFf-'
```

Parameters

ON
: Specifies that sessions from clients on AIX®, Linux, Mac OS X, and Solaris operating systems, where the users are not IBM Spectrum Protect authorized users, are prevented from initiating backup operations. This is the default. The server overrides the value for the BACKUPINITIATION parameter that is specified in the REGISTER NODE and UPDATE NODE commands.
Tip: For an overview of IBM Spectrum Protect authorized users, see UNIX and Linux client root and authorized user tasks.

OFf
: Specifies that the node value for the BACKUPINITIATION parameter is used. The BACKUPINITIATION parameter is specified in the REGISTER NODE and UPDATE NODE commands.

Example

Specify that the node value for the BACKUPINITIATION parameter is used.

```
backupinitiationroot off
```

CHECKTAPEPOS

The CHECKTAPEPOS option specifies whether the IBM Spectrum Protect™ server validates the position of data blocks on tape.

The CHECKTAPEPOS option applies only to operations that use tape drives. It does not apply to non-tape, sequential-access device classes such as FILE. If the server information about position does not match the position that is detected by the drive, an error message is displayed, the transaction is rolled back, and the data is not committed to the database.

Using the CHECKTAPEPOS option, you can enable append-only mode for IBM® LTO Generation 5 and later drives, and for any drives that support this feature. When it is enabled, the drive issues an error after it receives instructions to overwrite any data on the currently mounted volume. The IBM Spectrum Protect server repositions the tape to the correct block and continues writing data. Append-only mode provides added protection by preventing most data overwrite situations. If you are using a drive that supports this feature, you can validate data position on tape by using both IBM Spectrum Protect and the drive or you can enable one or the other.

Note: When you use SAN Tape acceleration functions in the fabric or SAN switch, set the CHECKTAPEPOS option to DRIVEonly or No to avoid false positive positioning errors. The IBM Spectrum Protect CHECKTAPEPOS server option does not require an append-only capable drive.

Changes to the CHECKTAPEPOS option affect mounts only after the update to the drive is complete.

The default is YES.

Syntax

```
>>-CHECKTAPEPOS--+-Yes-------+--------------------------------><
                 +-No--------+
                 +-TSMonly---+
                 '-DRIVEonly-'
```

Parameters

Yes
: Specifies that the IBM Spectrum Protect server validates data position on tape. For drives that support append-only mode, this parameter specifies that IBM Spectrum Protect enables the drive to also validate the data position during each WRITE operation to prevent data overwrite. Yes is the default.

No
: Specifies that all data position validation is turned off.

TSMonly

Specifies that the IBM Spectrum Protect server validates data position on tape. The server does not use append-only mode even if the drive supports the feature.

DRIVEonly
Specifies that the IBM Spectrum Protect server enables append-only mode for drives that support this feature. The server does not validate the data position on tape.

Example

Validate data position on tape and enable append-only mode for a supported drive:

```
checktapepos yes
```

CLIENTDEDUPTXNLIMIT

The CLIENTDEDUPTXNLIMIT option specifies the maximum size of a transaction when client-side deduplicated data is backed up or archived.

When you use client-side deduplication for large objects, intensive database activity can result from long-running transactions that are required to update the database. High levels of database activity can produce the following symptoms:

- Reduced throughput for client backup and archive operations
- Resource contention resulting from concurrent server operations
- Excessive recovery log activity

The extent to which these symptoms occur depends on the number and size of objects being stored using client-side data deduplication, the intensity and type of concurrent operations taking place on the IBM Spectrum Protect™ server, and the IBM Spectrum Protect server configuration.

With the CLIENTDEDUPTXNLIMIT server option, you can specify a maximum size, in gigabytes, for transactions when client-side deduplicated data is backed up or archived. If an object or set of objects in a single transaction exceeds the limit specified by CLIENTDEDUPTXNLIMIT, the objects are not deduplicated by the client, and the transaction can fail. You can specify a value 32 - 102400 GB. The default value is 5120 GB.

If an object or set of objects in a single transaction exceeds the limit specified by CLIENTDEDUPTXNLIMIT, the objects or set of objects is not deduplicated by the client. However, the objects are sent to the server. These objects can be deduplicated on the server, depending on whether the destination storage pool is configured for data deduplication and on the value of the SERVERDEDUPTXNLIMIT option. Objects in a deduplication-enabled storage pool that are less than the value of the SERVERDEDUPTXNLIMIT are deduplicated by a server duplicate-identification process.

The appropriate value for this option depends on the IBM Spectrum Protect server configuration and concurrent server activity. You can specify a high value for this option if you minimize resource contention. To minimize resource contention, perform operations, such as backup, archive, duplicate identification (the IDENTIFY DUPLICATES command), and reclamation, at different times.

To update this server option without stopping and restarting the server, use the SETOPT command.

Syntax

```
                        .-5120------.
>>-CLIENTDEDUPTXNlimit--+-gigabytes-+-------------------------><
```

Parameters

gigabytes
Specifies the maximum size, in gigabytes, of objects that can be backed up or archived using client-side data deduplication. You can specify a value 32 - 102400. The default value is 5120.

Examples

Disable client-side data deduplication for all objects over 80 GB:

```
clientdeduptxnlimit 80
```

CLIENTDEPLOYCATALOGURL

The CLIENTDEPLOYCATALOGURL option specifies the location of the catalog file that is used for automatic client deployment operations.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-CLIENTDEPLOYCATalogurl--------------------------------------->

   .-https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json-.
>--+-url-----------------------------------------------------------------------------------+-><
```

Parameters

url

Specifies the URL from which the server downloads the catalog file for automatic client deployment operations. The catalog file stores properties for client deployment operations, including the location of the deployment packages. The default URL is https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json.
To specify that the catalog file is downloaded from another location, use the SETOPT command to specify a custom URL. To reset the URL to the default value, issue the SETOPT command with an empty string: "". If you specify a custom URL, the custom URL is retained after the server is upgraded.

Example

Specify a custom URL of https://customAddress.

```
setopt clientdeploycatalogurl https://customAddress
```

Example

Restore the value of the CLIENTDEPLOYCATALOGURL option to the default.

```
setopt clientdeploycatalogurl ""
```

CLIENTDEPLOYUSELOCALCATALOG

The CLIENTDEPLOYCATALOGURL option specifies whether the local version of the catalog file is used for automatic client deployment operations.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
                                  .-No--.
>>-CLIENTDEPLOYUSELOCALcatalog--+-Yes-+------------------------><
```

Parameters

No

Specifies that the local version of the catalog file is not used. Instead, the catalog file is downloaded from the location that is specified by the CLIENTDEPLOYCATALOGURL option. The default value is NO.

Yes

Specifies that the local version of the catalog file is used. Catalog files are not downloaded during client deployment operations. If you set this option to YES, the value is retained after the server is upgraded.

Example

Specify that the local version of the catalog file is used.

```
setopt clientdeployuselocalcatalog yes
```

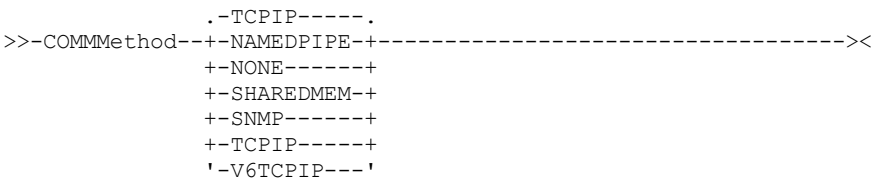
COMMMETHOD

The COMMMETHOD option specifies a communication method to be used by the server.

You can configure the server to use multiple communication methods. The more commonly used are the TCPIP, V6TCPIP, and SHAREDMEM communication methods. To specify multiple communication methods, enable each method by adding a COMMMETHOD stanza to the dsmserv.opt options file.

Important: When you enable a communication method, you must also add the options that are specific to the communication method to the options file.

Syntax



Parameters

You can choose one of the following communication methods:

Windows NAMEDPIPES
Windows Specifies the named pipes communication method option.

NONE
Specifies that no communication method is used. This option does not allow users to connect to the server and is useful for experimenting with policy commands.

SHAREDMEM
Specifies the shared memory communication method option. This method uses the same area of memory to send data between several applications at the same time. Both the server and the backup-archive client must be configured to support the shared memory communication method, and they must be installed on the same computer.

SNMP
Specifies the SNMP communication method option.

TCPIP
Specifies the TCP/IP communication method option. This option is the default. When TCPIP is specified, TCP/IP Version 4 is used exclusively.

V6TCPIP
Specifies the TCP/IP communication method option. If TCP/IP Version 4 and Version 6 are both configured, IBM Spectrum Protect™ uses both protocols simultaneously. If both COMMMETHOD TCPIP and COMMMETHOD V6TCPIP are specified, V6TCPIP overrides the specification of TCPIP. A valid domain name server (DNS) environment must be present to use either TCP/IP V4 or TCP/IP V6 if this option is specified.

Examples

Example of specifying multiple communication methods to be used by the server (TCP/IP and TCP/IP Version 6):

```
commmethod tcpip
commmethod v6tcpip
```

COMMTIMEOUT

The COMMTIMEOUT option specifies how long the server waits for an expected client message during an operation that causes a database update. If the length of time exceeds this time-out, the server ends the session with the client. You may want to increase the time-out value to prevent clients from timing out. Clients may time out if there is a heavy network load in your environment or they are backing up large files.

The COMMTIMEOUT server option is used for non-administrative sessions. See the ADMINCOMMTIMEOUT option for administrative client sessions.

You can update this server option without stopping and restarting the server by using the SETOPT command.

Syntax

```
                .-60------.
>>-COMMTimeout--+-seconds-+-----------------------------------><
```

Parameters

seconds
: Specifies the maximum number of seconds that a server waits for a client response. The default value is 60. The minimum value is 1.

Examples

```
commtimeout 60
```

AIX | Linux | Windows

CONTAINERRESOURCETIMEOUT

The CONTAINERRESOURCETIMEOUT option specifies how long the server waits to complete a data store operation to a container storage pool.

Syntax

When a timeout occurs, any data that was stored in the container storage pool remains there. The data store operation ends, and the request for the container resource is canceled.

```
                             .-180-----.
>>-CONTAINERRESOURCETimeout--+-minutes-+----------------------><
```

Parameters

minutes
: Specifies the maximum number of minutes that a server waits before an operation is canceled. The default value is 180 minutes. The minimum value is 1 minute.

Example

Specify that the server waits for 4 hours before a data store operation to a container storage pool is canceled.

```
containerresourcetimeout 240
```

Windows

DATEFORMAT

The DATEFORMAT option specifies the format in which dates are displayed by the server.

The DATEFORMAT value is overridden by the locale format if the locale is initialized at server startup. The locale is specified in the LANGUAGE option.

Syntax

```
>>-DATEformat--n-------------------------------------------------><
```

Parameters

n
: Select a number from 1 to 5 to identify the date format used by the server. The default value is 1.

  1
  : MM/DD/YYYY

  2
  : DD-MM-YYYY

  3
  : YYYY-MM-DD

  4
  : DD.MM.YYYY

  5
  : YYYY.MM.DD

Examples

```
dateformat 4
```

DBDIAGLOGSIZE

This option helps to control the amount of space that is used by diagnostic log files.

The database manager uses diagnostic log files to log messages. You must control the size of the log files so that they do not fill the file system. Use the DBDIAGLOGSIZE option to set the amount of space that is used by the log files.
If you set a value in the range 2 - 9999, a maximum of 10 rotating diagnostic log files are retained. Each file name indicates the order in which the file was created. After a file is full, the next file is created. When the 10th file is full, the oldest file is deleted, and a new file is created. The following example shows how the rotating log files might look:

```
db2diag.14.log, db2diag.15.log, ... , db2diag.22.log, db2diag.23.log
```

When db2diag.23.log is full, db2diag.14.log is deleted, and db2diag.24.log is created.
The server checks the file space that contains the diagnostic log files every hour. Messages are displayed every 12 hours if either of the following conditions occur:

- The available space in the file system where the diagnostic log files are located is less than 20% of the total file system space.
- The available space in the file system where the server instance directory is located is less than 1 GB.

If you specify a value of 0, only one log file, db2diag.log, is used for all diagnostic messages. No limits are imposed on the size of the log file.
Restriction: You must monitor the size of the diagnostic log files to ensure that they do not use all the available space in the file system. If there is not enough available space, the server might fail to respond.

Syntax

```
                    .-1024------.
>>-DBDIAGLOGSize--+-megabytes-+-------------------------------><
```

Parameters

megabytes
: Specifies the amount of space that is used by diagnostic log files in megabytes. Specify a value in the range 2 - 9999, or a value of 0. The default value is 1024.

If you specify a value in the range 2 - 9999, rotating log files are used, and the value specifies the total size in megabytes of all 10 log files. The value is reset to 1024 whenever the server is restarted.

If you specify a value of 0, one log file is used, and no limits are imposed on the size of the log file.

If you want to archive messages, specify a value of 0 to ensure that the db2diag.log file can use all the available space without using rotating log files.

After you set the value of the megabytes parameter to 0 by using the DBDIAGLOGSIZE option, messages are initially written to rotating log files. After the server is restarted, messages are written to the db2diag.log file.

Tip: If you specify a value in the range 2 - 9999 by using the server options file, dsmserv.opt, the value is not reset automatically at server startup. The value remains the same until it is changed or removed from the dsmserv.opt file, by using the SETOPT command.

Example: Specify a maximum size of 5120 megabytes

Specify the size of the diagnostic log files as 5120 megabytes (5 GB):

```
dbdiaglogsize 5120
```

Example: Archive messages in a single log file

Archive messages by specifying that the messages are written to the db2diag.log file:

```
dbdiaglogsize 0
```

Related information:
DB2 V10.5 product information

DBDIAGPATHFSTHRESHOLD

The DBDIAGPATHFSTHRESHOLD option specifies the threshold for free space on the file system or disk that contains the db2diag.log file.

When the amount of free space is equal to or less than the specified threshold, the ANR1545W error message is shown. By default, the message is shown when the file system or disk has 20% or less of free disk space.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-DBDIAGPATHFSTHreshold--percent-----------------------------><
```

Parameter

percent
Specifies the percentage of available space in the file system. Valid values are in the range 0 - 100. The default is 20.
Tip: For best results, do not set a low or high value for the percent parameter. A low value might cause the file system to become full before you can correct the issue. A full file system might corrupt the server database. A high value might result in many ANR1545W messages in the server activity log.

Example

Set the threshold value to 10%.

```
setopt DBDIAGPATHFSTH 10
```

DBMEMPERCENT

Use this option to specify the percentage of the virtual address space that is dedicated to the database manager processes.

If applications other than IBM Spectrum Protect™ server are running on the system, ensure that the value allows adequate memory for the other applications.

Syntax

```
>>-DBMEMPERCENT--+-percent-+-----------------------------------><
                 '-AUTO----'
```

Parameters

percent
: Set a value from 10 to 99.

AUTO
: The database manager sets the percentage automatically to a value that is between 75 percent and 95 percent of system RAM. The default value is AUTO.

Examples

```
dbmempercent 50
```

DBMTCPPORT

The DBMTCPPORT option specifies the port number on which the TCP/IP communication driver for the database manager waits for requests for client sessions.

The specified port number must be reserved for use by the database manager.

By default, the IBM Spectrum Protect™ server uses interprocess communications (IPC) to establish connections for the first two connection pools, with a maximum of 480 connections for each pool. After the first 960 connections are established, the IBM Spectrum Protect server uses TCP/IP for any additional connections.

Syntax

```
>>-DBMTCPPort--port_number-------------------------------------><
```

Parameters

port_number
: Specifies the number of the TCP/IP port on which the database manager waits for communications from the server. Valid values are integers from 1024 to 65535.

  The default port number is the value of the server TCPPORT option plus 50,000. For example, if the server TCPPORT option is 1500, the default DBMTCPPORT port number would be 51500.

  If the TCPPORT server option is greater than 9999, add the last four digits of its value to 50000. For example, if the TCPPORT option is 11500, 1550 is added to 50000, resulting in a DBMTCPPORT port number of 51500.

Example

```
dbmtcpport 51500
```

DEDUPREQUIRESBACKUP

The DEDUPREQUIRESBACKUP option specifies whether volumes in primary sequential-access storage pools that are set up for data deduplication can be reclaimed and whether duplicate data can be discarded before the storage pools are backed up.

If the value of this option is YES (the default), you must back up data to copy storage pools that are not set up for data deduplication. Use the BACKUP STGPOOL command to back up data to copy storage pools.

Be aware that reclamation of a volume in a storage pool that is set up for data deduplication might not occur when the volume first becomes eligible. The server makes additional checks to ensure that data from a storage pool that is set up for data deduplication has been backed up to a copy storage pool. These checks require more than one BACKUP STGPOOL instance before the server reclaims a volume. After the server verifies that the data was backed up, the volume is reclaimed.

You can change this option dynamically using the SETOPT command.

Attention: To minimize the possibility of data loss, do not change the default setting for this server option. Specify a value of NO only if you do not have any copy storage pools and are not performing storage pool backups.

Syntax

```
>>-DEDUPREQUIRESBACKUP--+-Yes-+--------------------------------><
                        '-No--'
```

Parameters

Yes
: Specifies that the storage pool must be backed up before volumes can be reclaimed and before duplicate data can be discarded. This is the default.

No
: Specifies that volumes in primary sequential-access storage pools that are set up for data deduplication can be reclaimed and duplicate data can be discarded if the storage pools are not backed up.

Examples

Specify that primary sequential-access storage pools that are set up for data deduplication do not have to be backed up.

```
deduprequiresbackup no
```

DEDUPTIER2FILESIZE

The DEDUPTIER2FILESIZE option specifies at what file size IBM Spectrum Protect™ begins to use Tier 2 data deduplication.

Syntax

```
>>-DEDUPTIER2FILESIZE--nnn-------------------------------------><
```

Parameters

nnn
: Specifies the file size, in gigabytes, at which point the IBM Spectrum Protect server begins to use Tier 2 processing for data deduplication. You can specify a value 20 - 9999. The default is 100.
Note: If the value specified or defaulted to for this option is greater than the value for the SERVERDEDUPTXNLIMIT option, then this option is ignored for server data deduplication. If the value specified or defaulted to for this option is greater than the value for CLIENTDEDUPTXNLIMIT, then this option is ignored for client data deduplication.

Examples

```
deduptier2filesize 550
```

DEDUPTIER3FILESIZE

The DEDUPTIER3FILESIZE option specifies at what file size IBM Spectrum Protect™ begins to use Tier 3 data deduplication.

Syntax

```
>>-DEDUPTIER3FILESIZE--nnn-------------------------------------><
```

Parameters

nnn
: Specifies the file size, in gigabytes, at which point the IBM Spectrum Protect server begins to use Tier 3 processing for data deduplication. You can specify a value 90 - 9999. The default is 400.

  - If the value specified or defaulted to for this option is greater than the value for the SERVERDEDUPTXNLIMIT option, then this option is ignored for server data deduplication.
  - If the value specified or defaulted to for this option is greater than the value for CLIENTDEDUPTXNLIMIT, then this option is ignored for client data deduplication.
  - If the value specified or defaulted to for this option is less than the value specified or defaulted to for DEDUPTIER2FILESIZE, then the value of DEDUPTIER2FILESIZE is used for this option.

Examples

```
deduptier3filesize 1150
```

DEVCONFIG

The DEVCONFIG option specifies the name of a file in which you want IBM Spectrum Protect™ to store a backup copy of device configuration information.

IBM Spectrum Protect stores the following information in the device configuration file:

- Device class definitions created by using the DEFINE DEVCLASS command
- Drive definitions created by using the DEFINE DRIVE command
- Library definitions created by using the DEFINE LIBRARY command
- Library inventory information for the LIBTYPE=SCSI automated libraries
- Path definitions created by using the DEFINE PATH command
- Server definitions created with the DEFINE SERVER command
- Server name created with the SET SERVERNAME command
- Server password created with the SET SERVERPASSWORD command

Note:

- Only path definitions with SRCTYPE=SERVER are backed up to the device configuration file. Paths of SRCTYPE=DATAMOVER are not written to the file.
- Library volume location information is stored as comments (/*...*/) in the device configuration file whenever CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME, and AUDIT LIBRARY commands are issued for SCSI libraries.

Attention: To restore the database after a disaster, you must have a copy of the current device configuration file. The device configuration file cannot be recreated.

You can include one or more DEVCONFIG options in the server options file. When you use multiple DEVCONFIG options, IBM Spectrum Protect automatically updates and stores a backup copy of device configuration information in each file you specify.

Syntax

```
>>-DEVCONFig--file_name-----------------------------------------><
```

Parameters

file_name
: Specifies the name of a file in which to store a backup copy of device configuration information.

Examples

```
devconfig devices.sav
```

DISABLEREORGTABLE

The DISABLEREORGTABLE option specifies whether online table reorganization is disabled for table names that are specified in the tables list.

To use the DISABLEREORGTABLE option, you must halt the server, update the options file, and then restart the server.

Syntax

```
>>-DISABLEREORGTable----tablelist------------------------------><
```

Parameters

tablelist
: Specifies a list of table names for which table reorganization is disabled. If you do not specify any table names with the option, or if the option is not in the options file, no tables are disabled.
Restriction: The following tables are already excluded from table reorganization processing and cannot be specified for this option:

- STAGED_EXPIRING_OBJECTS
- STAGED_OBJECT_IDS
- BF_DEREFERENCED_CHUNKS
- BF_QUEUED_CHUNKS

Example

```
DISABLEREORGTABLE BF_BITFILE_EXTENTS,REPLICATING_OBJECTS
```

DISABLESCHEDS

The DISABLESCHEDS option specifies whether administrative and client schedules are disabled during IBM Spectrum Protect™ server recovery.

Syntax

```
>>-DISABLESCheds--+-Yes-+-------------------------------------><
                  '-No--'
```

Parameters

Yes
: Specifies that administrative and client schedules are disabled.

No
: Specifies that administrative and client schedules are enabled.

Examples

```
disablescheds no
```

DISPLAYLFINFO

The DISPLAYLFINFO option specifies how the accounting records and summary table entries report the node name.

When this option is enabled, the accounting records and summary table entries report node_name(storage_agent_name) for the node name. If the option is not enabled, the accounting records and summary table entries simply report node_name for the node name. The default is No.

Syntax

```
>>-DISPLAYLFINFO--+-Yes-+-------------------------------------><
                  '-No--'
```

Parameters

Yes
: Specifies that the accounting records and summary table entries will report the storage agent name.

No
: Specifies that the accounting records and summary table entries will not report the storage agent name. This is the default.

Examples

```
displaylfinfo yes
```

The result shows the following accounting record with the storage agent name displayed (STA53):

```
5,0,ADSM,07/13/2004,15:35:14,COLIND-TUC(STA53),,WinNT,1,Tcp/Ip,1,0,0,0,
0,223,4063,0,0,222,7,8,3,1,4,0,0,0,0,3,0
```

The corresponding summary table also displays the storage agent name:

```
      START_TIME: 2004-07-13 15:35:07.000000
        END_TIME: 2004-07-13 15:35:14.000000
        ACTIVITY: BACKUP
          NUMBER: 8
          ENTITY: COLIND-TUC(STA53)
        COMMMETH: Tcp/Ip
         ADDRESS: colind-tuc:2229
   SCHEDULE_NAME:
        EXAMINED: 0
        AFFECTED: 223
          FAILED: 0
           BYTES: 4160875
            IDLE: 8
          MEDIAW: 1
      PROCESSES: 1
     SUCCESSFUL: YES
    VOLUME_NAME:
     DRIVE_NAME:
   LIBRARY_NAME:
       LAST_USE:
      COMM_WAIT: 3
NUM_OFFSITE_VOLS:
```

DNSLOOKUP

The DNSLOOKUP option specifies whether the server uses system API calls to determine the domain name server (DNS) names of systems that contact the server.

Syntax

```
>>-DNSLOOKUP--+-Yes-+----------------------------------------><
              '-No--'
```

Parameters

Yes

Specifies that the server obtains the DNS names of contacting systems. Yes is the default.

No
Specifies that the server does not obtain the DNS names of contacting systems.

Examples

```
dnslookup yes
```

DRIVEACQUIRERETRY

The DRIVEACQUIRERETRY option lets you specify how many times the server retries the acquisition of a drive in an IBM® 349x library. If the library is shared among multiple applications, its drives may appear to be available to the server (through the use of a background polling process) when they are not.

This option is only valid if you specified 3494SHARED YES in the dsmserv.opt file. If you specified DRIVEACQUIRERETRY NEVER, you need to monitor how long jobs have been waiting for drives and how long the server has been polling the drives. You may also need to check the status of these drives in the other IBM Spectrum Protect™ servers. There may be cartridges stuck in the drives, and the other IBM Spectrum Protect servers may have marked the drives as *offline*. If this is the case, you need to mark the drives *offline* in the IBM Spectrum Protect server that is polling the drives. If necessary, also cancel any waiting jobs.

Syntax

```
>>-DRIVEACQuireretry--+-Forever-----------+------------------><
                      +-Never-------------+
                      '-number_of_retries-'
```

Parameters

Forever
The acquisition of a drive is retried until one is successfully acquired. This is the default.

Never
The server does not retry the acquisition of a drive and fails the operation.

number_of_retries
Specifies the maximum number of times, from 1 to 9999, that the server retries the acquisition of a drive.

Examples

Specify that the server should attempt no more than 10 times to acquire the drive:

```
driveacquireretry 10
```

ENABLENASDEDUP

The ENABLENASDEDUP server option specifies whether the server deduplicates data that is stored by a network-attached storage (NAS) file server. This option applies only to NetApp file servers.

If the value of this option is NO, the data stored by the file server is skipped during duplicate-identification processing. If the value of this option is YES, the value of the DEDUPLICATE parameter in the storage pool definition must be YES.

Syntax

```
>>-ENABLENASDEDUP--+-No--+-------------------------------------><
                   '-Yes-'
```

Parameters

Yes
Specifies that IBM Spectrum Protect™ server deduplicates data stored by a NetApp file server.

No
Specifies that the server does not deduplicate data stored by a NetApp file server.

Example

Specify that the server deduplicates data stored by a NetApp file server.

```
enablenasdedup yes
```

EVENTSERVER

The EVENTSERVER option specifies whether at startup the server should try to contact the event server.

Syntax

```
>>-EVENTSERVer--+-Yes-+----------------------------------------><
                '-No--'
```

Parameters

Yes
Specifies that, at startup, the server tries to contact the event server. Contact occurs only if a DEFINE EVENTSERVER command has already been issued. This is the default.
No
Specifies that, at startup, the server does not try to contact the event server.

Examples

```
eventserver yes
```

EXPINTERVAL

The EXPINTERVAL option specifies the interval, in hours, between automatic inventory expiration processes by IBM Spectrum Protect™. Inventory expiration removes client backup and archive file copies from the server as specified by the management classes to which the client files are bound. If expiration is not run periodically, storage pool space is not reclaimed from expired client files, and the server requires more storage space than required by policy.

You can also use the EXPIRE INVENTORY command to start inventory expiration. Expiration can make space available in your storage pools for additional client backup or archive files.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
                .-24----.
>>-EXPINterval--+-hours-+----------------------------------------><
```

Parameters

hours
Specifies the time, in hours, between automatic inventory expiration processes. You can specify from 0 to 336 (14 days). A value of 0 means that expiration must be started with the EXPIRE INVENTORY command. The default is 24.

Examples

```
expinterval 5
```

EXPQUIET

The EXPQUIET option specifies whether IBM Spectrum Protect™ sends detailed messages during expiration processing.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-EXPQUiet--+- --No--+---------------------------------------><
             '- --Yes-'
```

Parameters

No
: Specifies that the server sends detailed messages. This is the default.

Yes
: Specifies that the server sends only minimal messages. These messages are sent only for files that have expired based on the copy group in the default management class or retention grace period for the domain.

Examples

```
expquiet no
```

Linux

FASPBEGPORT

The FASPBEGPORT option specifies the starting number in the range of port numbers that are used for network communications with Aspera® Fast Adaptive Secure Protocol (FASP®) technology.

To define the range of port numbers, specify both the FASPBEGPORT and FASPENDPORT options.

Syntax

```
                .-15100----------------.
>>-FASPBEGPort--+-starting_port_number-+----------------------><
```

Parameters

starting_port_number
: Specifies the starting port number for network communications that use Aspera FASP technology. The default value is 15100.
Ask your network administrator to help you define the range of port numbers:

- If you did not enable the Secure Sockets Layer (SSL) protocol for the server pair, ensure that the ports can be used for Transmission Control Protocol (TCP) sockets.
- Ensure that the ports can be used for User Datagram Protocol (UDP) connections.
- Ensure that the ports are compatible with firewall rules.

Example

If firewall rules require port numbers to be greater than 1800, you would specify a minimum port number of 1801:

```
faspbegport 1801
```

Related reference:
FASPENDPORT

Linux

FASPENDPORT

The FASPENDPORT option specifies the ending number in the range of port numbers that are used for network communications with Aspera® Fast Adaptive Secure Protocol (FASP®) technology.

To define the range of port numbers, specify both the FASPBEGPORT and FASPENDPORT options.

Syntax

```
                .-15199--------------.
>>-FASPENDPort--+-ending_port_number-+------------------------><
```

Parameters

ending_port_number
: Specifies the ending port number for network communications that use Aspera FASP technology. The default value is 15199.
Ask your network administrator to help you define the range of port numbers:

- If you did not enable the Secure Sockets Layer (SSL) protocol for the server pair, ensure that the ports can be used for Transmission Control Protocol (TCP) sockets.
- Ensure that the ports can be used for User Datagram Protocol (UDP) connections.
- Ensure that the ports are compatible with firewall rules.

Example

If firewall rules require port numbers to be less than 1900, you would specify a maximum port number of 1899:

```
faspendport 1899
```

Related reference:
FASPBEGPORT
Linux

FASPTARGETRATE

The FASPTARGETRATE option specifies the target rate for data transfer with Aspera® Fast Adaptive Secure Protocol (FASP®) technology. By specifying the target rate, you limit the bandwidth of each network connection that uses Aspera FASP technology. In this way, you can ensure that sufficient bandwidth is available for all network connections.

Syntax

```
                  .-250000------.
>>-FaspTargetRate--+-target_rate-+----------------------------><
```

Parameters

target_rate
: Specifies the maximum rate, in kilobits per second, for data transfer during a session. The default value is 250000. You can specify values in the range 100 - 100000000.

For example, if you issue the PROTECT STGPOOL command to run two parallel operations at the default target rate, the aggregated throughput does not exceed 500,000 kbps. If your file system can support two operations to protect storage pools at much higher rates than 500,000 kbps of aggregated throughput, and sufficient network bandwidth is available, you can increase the target rate.

To determine the appropriate target rate, consult your network administrator.

Examples

If the allotted network bandwidth is 150,000 kbps, you can set the target rate to 75,000 and use the default number of sessions (two) for the PROTECT STGPOOL command.

```
fasptargetrate 75000
```

In a large blueprint configuration, if the allotted network bandwidth is 6,000,000 kbps, you can set the target rate to 750,000 and use eight sessions for the PROTECT STGPOOL command.

```
fasptargetrate 750000
```

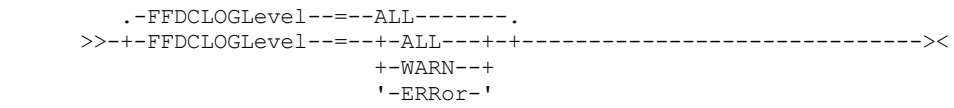
FFDCLOGLEVEL

The FFDCLOGLEVEL option specifies the type of general server messages that are displayed in the first failure data capture (FFDC) log.

The FFDC log contains three categories of general server messages. Setting the FFDCLOGLEVEL option affects the following categories:

- FFDC_GENERAL_SERVER_INFO
- FFDC_GENERAL_SERVER_WARNING
- FFDC_GENERAL_SERVER_ERROR

Syntax



Parameters

ALL

Specifies that all FFDC general server log messages are in the log. This value is the default.

WARN

Specifies that the FFDC_GENERAL_SERVER_WARNING and FFDC_GENERAL_SERVER_ERROR messages appear in the log.

ERRor

Specifies that only the FFDC_GENERAL_SERVER_ERROR messages appear in the log.

Example

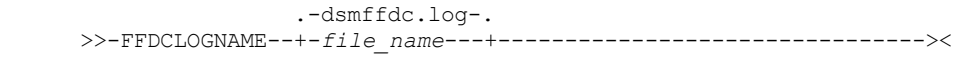
```
ffdcloglevel warn
```

FFDCLOGNAME

The FFDCLOGNAME option specifies a name for the first failure data capture (FFDC) log.

The FFDC log file is used to gather diagnostic information about the server. When an error occurs, data about the error is written to the FFDC log file. This information can be provided to IBM Support to help diagnose problems. The FFDC log file is in the server instance directory.

Syntax



Parameters

file_name
Specifies a file name for the FFDC log file. The file name can be a fully qualified file name or a file name relative to the server instance directory. The default value is dsmffdc.log.

Examples

```
ffdclogname /tsminst1/tsmffdc.log
ffdclogname tsmffdc.log
ffdclogname c:\tsmserv1\tsmffdc.log
```

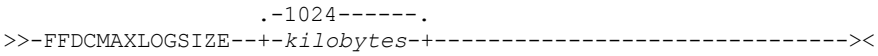
Related reference:
FFDCMAXLOGSIZE
FFDCNUMLOGS

FFDCMAXLOGSIZE

The FFDCMAXLOGSIZE option specifies the size for the first failure data capture (FFDC) log file.

The FFDC log file is used to gather diagnostic information about the server. When an error occurs, data about the error is written to the FFDC log file. This information can be provided to IBM Support to help diagnose problems.

Syntax



Parameters

kilobytes
Specifies the size to which the FFDC log file can grow before wrapping. The minimum value is 500. The maximum value is 2097151. The default value is 1024.

To allow the size of the log file to grow indefinitely, specify a value of -1. To disable the log, specify 0.

Examples

```
ffdcmaxlogsize 2000
```

Related reference:
FFDCLOGNAME
FFDCNUMLOGS

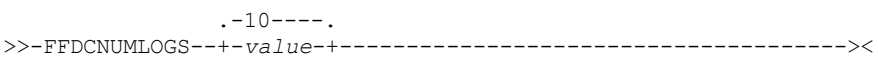
FFDCNUMLOGS

The FFDCNUMLOGS option specifies the number of log files that can be used for circular logging. The default value is 10.

Circular logging uses a ring of log files to provide recovery from transaction failures and system crashes. For example, when the dsmffcd.log file is full, it is renamed to dsmffdc.log.1. If a dsmffdc.log.1 file exists, the dsmffdc.log.1 file is renamed to dsmffdc.log.2. If a dsmffdc.log.2 exists, the dsmffdc.log.2 file is renamed to dsmffdc.log.3, and so on, until the FFDCNUMLOGS value is reached. If there is a log file that is renamed as the FFDCNUMLOGS value is reached, that log file is deleted.

The minimum value is 1. The maximum value is 100. The default value is 10.

Syntax



Parameters

value
Specifies the number of log files that are used for circular logging.

If you specify a value of 1 and the log file size reaches the FFDCMAXLOGSIZE, the server continues to write to the log file. Any logging information is overwritten and the server continues to write to the log file.

Examples

```
ffdcnumlogs 20
```

FILEEXIT

The FILEEXIT option specifies a file to which enabled events are routed. Each logged event is a record in the file.

Syntax

```
>>-FILEEXIT--+-No--+--file_name--+-REPLACE--+-----------------><
             '-Yes-'             +-APPEND---+
                                 '-PRESERVE-'
```

Parameters

Yes
Specifies that event logging to the file exit receiver begins automatically at server startup.

No
Specifies that event logging to the file exit receiver does not begin automatically at server startup. When this parameter has been specified, you must begin event logging manually by issuing the BEGIN EVENTLOGGING command.

file_name
Specifies the name of the file in which the events are stored.

REPLACE
Specifies that if the file already exists, it will be overwritten.

APPEND
Specifies that if the file already exists, data is appended to it.

PRESERVE
Specifies that if the file already exists, it will not be overwritten.

Examples

Windows

```
fileexit yes \tsm\server\data replace
```

AIX | Linux

```
fileexit yes /tsm/server/data replace
```

FILETEXTEXIT

The FILETEXTEXIT option specifies a file to which enabled events are routed. Each logged event is a fixed-size, readable line.

Syntax

```
>>-FILETEXTEXIT--+-No--+--file_name--+-REPLACE--+--------------><
                 '-Yes-'             +-APPEND---+
                                     '-PRESERVE-'
```

Parameters

Yes

Specifies that event logging to the file exit receiver begins automatically at server startup.

No
: Specifies that event logging to the file exit receiver does not begin automatically at server startup. When this parameter has been specified, you must begin event logging manually by issuing the BEGIN EVENTLOGGING command.

file_name
: Specifies the name of the file in which the events are stored.

REPLACE
: Specifies that if the file already exists, it will be overwritten.

APPEND
: Specifies that if the file already exists, data will be appended to it.

PRESERVE
: Specifies that if the file already exists, it will not be overwritten.

Examples

Windows

```
filetextexit yes \tsm\server\data replace
```

AIX | Linux

```
filetextexit yes /tsm/server/data replace
```

FIPSMODE

The FIPSMODE option specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for non-Secure Sockets Layer (SSL) operations.

Syntax

```
   .-FIPSMODE--=--No------.
>>-+----------------------+-----------------------------------><
   '-FIPSMODE--=--+-No--+-'
                  '-Yes-'
```

Parameters

No
: Specifies that FIPS mode is not enforced on the server for non-SSL operations. The default is NO.

Yes
: A value of YES indicates that FIPS mode is enforced on the server. This setting restricts cryptographic operations that involve object data, authentication, and passwords to use FIPS-approved cipher suites. The value does not affect SSL session operations, which are controlled by using the SSLFIPSMODE option.

Example: Enable FIPS mode on the server

```
fipsmode yes
```

Example: Enable FIPS mode and SSLFIPS mode on the server

```
fipsmode yes
sslfipsmode yes
```

FSUSEDTHRESHOLD

The FSUSEDTHRESHOLD option specifies what percentage of the file system can be filled up by the database before an alert message is issued.

You can update this server option without stopping and restarting the server by using the SETOPT command.

If this value is set to a low number, the activity log might be flooded with messages about the database space being filled, even if there is still space available. If the value is set too high, the database space might be filled before you can add more space to the file system.

Syntax

```
>>-FSUSEDTHreshold--percent-----------------------------------><
```

Parameters

percent
: Specifies the value of used space in the database. You can specify a value from 0 to 100. The default is 90.

Examples

```
fsusedthreshold 70
```

IDLETIMEOUT

The IDLETIMEOUT option specifies the amount of time, in minutes, that a client session can be idle before the server cancels the session. You may want to increase the time-out value to prevent clients from timing out if there is a heavy network load in your environment. Note, however, that a large number of idle sessions could prevent other users from connecting to the server.

The IDLETIMEOUT server option is used for non-administrative sessions. See the ADMINIDLETIMEOUT option for administrative client sessions.

You can update this server option without stopping and restarting the server by using the SETOPT command.

Syntax

```
                .-15------.
>>-IDLETimeout--+-minutes-+-----------------------------------><
```

Parameters

minutes
: Specifies the maximum number of minutes that a server waits for an idle client. The default value is 15 minutes. The minimum value is 1 minute.

Examples

```
idletimeout 15
```

KEEPALIVE

The KEEPALIVE option specifies whether the Transmission Control Protocol (TCP) keepalive function is enabled for outbound TCP sockets. The TCP keepalive function sends a transmission from one device to another to check that the link between the two devices is operating.

If you are using node replication, you can use the KEEPALIVE option on the source replication server to enable the TCP keepalive function. The KEEPALIVE option is not required on the target replication server unless you specify bidirectional replication, in which case the target server becomes the source replication server.

Syntax

```
              .-Yes-.
```

```
>>-KEEPALIVE--+-No--+-----------------------------------------><
```

Parameters

Yes
: Specifies that the TCP keepalive function is enabled for outbound TCP sockets. This value is the default.
If the KEEPALIVE option is enabled, default values are used for the KEEPALIVETIME and KEEPALIVEINTERVAL options.

No
: Specifies that the TCP keepalive function is not enabled for outbound TCP sockets.
If you specify a value of NO, it does not affect current TCP socket connections that originated from outbound connection requests while the KEEPALIVE option was set to YES. The YES value applies to those sockets until the related session ends and the socket is closed.

Example

Use the SETOPT command to enable the keepalive function without disabling or halting the server:

```
setopt keepalive yes
```

Related reference:
KEEPALIVEINTERVAL
KEEPALIVETIME

KEEPALIVETIME

The KEEPALIVETIME option specifies how often TCP sends a keepalive transmission when it receives a response. This option applies only if you set the KEEPALIVE option to YES.

Syntax

```
                  .-300-----.
>>-KEEPALIVETIME--+-seconds-+---------------------------------><
```

Parameters

seconds
: Specifies how often TCP sends keepalive transmissions to verify that an idle connection is still active. The value is specified in seconds.
You can specify a value in the range 1 - 4294967. The default is 300 (5 minutes).

Example

Set the KEEPALIVETIME option to 120 seconds:

```
keepalivetime 120
```

Related reference:
KEEPALIVE
KEEPALIVEINTERVAL

KEEPALIVEINTERVAL

The KEEPALIVEINTERVAL option specifies how often a keepalive transmission is sent if no response is received. This option applies only if you set the KEEPALIVE option to YES.

Syntax

```
                     .-30------.
```

```
>>-KEEPALIVEINTERVAL--+-seconds-+-----------------------------><
```

Parameters

seconds
: Specifies the length of time, in seconds, between keepalive transmissions when no response is received. The value is specified in seconds.
You can specify a value in the range 1 - 4294967. The default is 30 seconds.

Example

Set the KEEPALIVEINTERVAL option to 45 seconds:

```
keepaliveinterval 45
```

Related reference:
KEEPALIVE
KEEPALIVETIME

LANGUAGE

The LANGUAGE option controls the initialization of locales. A locale includes the language and the date, time, and number formats to be used for the console and server.

If your client and server are running different languages, the messages that are generated might not be understandable when messages are issued from the client to the server or if the server sends output to the client.

AIX | Linux If initialization of the locale fails, the server defaults to American English.

Windows If the initialization of the locale fails, the server defaults to American English and uses the date, time, and number formats that are set by the DATEFORMAT, TIMEFORMAT, and NUMBERFORMAT server options.

Syntax

```
                    (1)
>>-LANGuage--+-AMENG------+-----------------------------------><
             |       (2)   |
             +-en_US------+
             |         (3) |
             '-locale-----'
```

Notes:

1. AMENG is available only on HP-UX, Solaris, Windows.
2. en_US is available only on AIX and Linux.
3. *locale* is available only on AIX, HP-UX, Solaris, Linux, and Windows.

Parameters

Windows AMENG
: Windows Specifies that American English is used as the default language for the server.

AIX | Linux en_US
: AIX | Linux Specifies that American English is used as the default language for the server.

locale
: Specifies the name of the locale that is supported by the server. See the following tables for information on supported locales by operating system.
Note: IBM Spectrum Protect™ runs in any locale, but defaults to American English. For the locales listed, language support is available.

AIX

Table 1. Server languages for AIX®

Language	LANGUAGE option value
Chinese, Simplified	zh_CN
Chinese, Simplified	Zh_CN
Chinese, Simplified (UTF-8)	ZH_CN
Chinese, Traditional (Big5)	Zh_TW
Chinese, Traditional (UTF-8)	ZH_TW
Chinese, Traditional (euc_tw)	zh_TW
English	en_US
English (UTF-8)	EN_US
French	fr_FR
French (UTF-8)	FR_FR
German	de_DE
German (UTF-8)	DE_DE
Italian	it_IT
Italian (UTF-8)	IT_IT
Japanese, EUC	ja_JP
Japanese, PC	Ja_JP
Japanese, UTF8	JA_JP
Korean	ko_KR
Korean (UTF-8)	KO_KR
Portuguese, Brazilian	pt_BR
Portuguese, Brazilian (UTF-8)	PT_BR
Russian	ru_RU
Russian (UTF-8)	RU_RU
Spanish	es_ES
Spanish (UTF-8)	ES_ES
Table note: The system must have en_US environment support installed.	

Linux

Table 2. Server languages for Linux

LANGUAGE	LANGUAGE option value
Chinese, Simplified	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinese, Traditional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
English, United States	en_US
	en_US.utf8
French	fr_FR
	fr_FR.utf8
German	de_DE
	de_DE.utf8

LANGUAGE	LANGUAGE option value
Italian	it_IT
	it_IT.utf8
Japanese	ja_JP
	ja_JP.utf8
Korean	ko_KR
	ko_KR.utf8
Portuguese, Brazilian	pt_BR
	pt_BR.utf8
Russian	ru_RU
	ru_RU.utf8
Spanish	es_ES
	es_ES.utf8

Windows

Table 3. Server languages for Windows

Language	LANGUAGE option value
Chinese, Simplified	chs
Chinese, Traditional	cht
English	ameng
French	fra
German	deu
Italian	ita
Japanese	jpn
Korean	kor
Portuguese, Brazilian	ptb
Russian	rus
Spanish	esp

Examples

AIX Linux

```
lang ja_JP
```

Windows

```
lang jpn
```

LDAPCACHEDURATION

The LDAPCACHEDURATION option determines the amount of time that the IBM Spectrum Protect™ server caches LDAP password authentication information.

After a successful LDAP bind, the value that you enter determines the amount of time that information about the LDAP directory server is kept available. The higher the number, the better the performance of the LDAP directory server. During the cache period, though, changes on the LDAP directory server do not take immediate effect on the node. For example, old passwords might be available for some time, even after they were changed or locked on the LDAP server.

Include the LDAPCACHEDURATION option in a SETOPT command to have the option take effect immediately.

Restriction: The LDAPCACHEDURATION option does not apply to storage agents.

Syntax

```
>>-LDAPCACHEDURATION--minutes----------------------------------><
```

Parameters

minutes
: Specifies the maximum amount of time after a successful LDAP bind, that subsequent sessions to the same node or administrator skip secondary LDAP bind operations. Values range from zero to 360 minutes.

Example: Set the LDAPCACHEDURATION value to 6 hours (maximum)

In the dsmserv.opt file, specify the following value:

```
ldapcacheduration 360
```

After a node or administrator authenticates with an external directory server, the LDAP bind is skipped for 360 minutes on all sessions.

LDAPURL

The LDAPURL option specifies the location of a Lightweight Directory Access Protocol (LDAP) server. Set the LDAPURL option after you configure the LDAP server.

Tip: The information in this documentation applies to the LDAP authentication method that is preferred for IBM Spectrum Protect™ V7.1.7 or later servers. For instructions about using the previous LDAP authentication method, see Managing passwords and logon procedures.
The following restrictions apply:

- The LDAPURL option cannot be used in combination with the SETOPT command.
- The LDAPURL option does not apply to storage agents.

Syntax

```
>>-LDAPURL--ldap_url_value-------------------------------------><
```

Parameters

ldap_url_value
: Specifies the URL of one LDAP server, or the URLs of multiple LDAP servers. You can enter multiple values, with each URL value up to 1024 characters. The port number is optional and defaults to 389. Each URL value must contain an LDAP server name. For example, the format of the server name is `server1.storage.us.ibm.com` and the LDAP port is `341`. The value of the LDAPURL option must conform to the following specifications:

  - If you specify multiple URLs, each URL must be on a separate line.
  - If you specify multiple URLs, each URL must point to a different external directory, and all external directories must contain the same data.
  - Each URL must begin with `ldap://`.
    Restriction: The URL that you designate cannot begin with ldaps://.

    IBM Spectrum Protect supports LDAP connections that are secured with the standard LDAPv3 StartTLS operation, which establishes a secure Transport Layer Security (TLS) exchange on an existing LDAP connection. The LDAP Simple Bind operation that IBM Spectrum Protect uses does not protect the password when it is sent. A secure TLS connection is required to protect the password.

Example: Set the port value for an LDAP server

In the dsmserv.opt file, specify the port value as 341 for an LDAP server:

```
ldapurl ldap://server1.storage.us.ibm.com:341/dc=storage,dc=us,dc=ibm,dc=com
```

MAXSESSIONS

The MAXSESSIONS option specifies the maximum number of simultaneous client sessions that can connect with the server.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
                .-25-----------------.
>>-MAXSessions--+-number_of_sessions-+------------------------><
```

Parameters

number_of_sessions
: Specifies the maximum number of simultaneous client sessions. The default value is 25 client sessions. The minimum value is 2 client sessions. The maximum value is limited only by available virtual storage size or communication resources.

Examples

```
maxsessions 25
```

MESSAGEFORMAT

The MESSAGEFORMAT option specifies whether a message number is displayed in all lines of a multi-line message.

Syntax

```
>>-MESsageformat--number---------------------------------------><
```

Parameters

number
: Select a number to specify if a message number is to be displayed only on the first line of a multi-line message or is to be displayed on all lines.

  1
  : The message number for a message is displayed only in the first line of the message. This is the default.

  2
  : The message number for a message is displayed in all lines of a message.

Examples

```
messageformat 2
```

MIRRORLOGDIRECTORY

The MIRRORLOGDIRECTORY option specifies the directory for mirroring the active log path.

All changes made to the active log directory are also written to this mirror directory. This option is appended to the options file when the DSMSERV FORMAT command is run. Typically, the directory does not need to be changed.

Syntax

```
>>-MIRRorlogdirectory--dir_name--------------------------------><
```

Parameters

dir_name
: Specifies a fully qualified directory name for the active log mirror. The maximum number of characters is 175.

Examples

AIX Linux

```
mirrorlogdirectory /tsm/mirrorlog
```

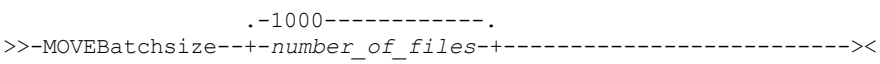
Windows

```
mirrorlogdirectory c:\tsmserv1\mirrorlog
```

MOVEBATCHSIZE

The MOVEBATCHSIZE option specifies the number of client files that are to be moved and grouped together in a batch, within the same server transaction. This data movement results from storage pool backups and restores, migration, reclamation, and MOVE DATA operations. This option works with the MOVESIZETHRESH option.

Syntax



Parameters

number_of_files
: Specifies a number of files between 1 and 1000. The default is 1000.

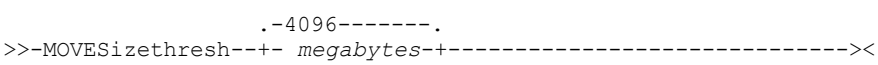
Examples

```
movebatchsize 100
```

MOVESIZETHRESH

The MOVESIZETHRESH option specifies, in megabytes, a threshold for the amount of data moved as a batch, within the same server transaction. When this threshold is reached, no more files are added to the current batch, and a new transaction is started after the current batch is moved.

Syntax



Parameters

megabytes
: Specifies the number of megabytes as an integer from 1 to 32768. The default value is 4096. This option is used with the MOVEBATCHSIZE option.

Examples

```
movesizethresh 500
```

MSGINTERVAL

The MSGINTERVAL option specifies the time, in minutes, between messages prompting an operator to mount a tape for the server.

Syntax

```
                .-1-------.
>>-MSGINTerval--+-minutes-+-------------------------------------><
```

Parameters

minutes
: Specifies the time interval at which the operator is prompted by the server to mount a tape. The default value is 1 minute. The minimum value is 1 minute.

Examples

```
msginterval 2
```

Windows

NAMEDPIPENAME

The NAMEDPIPENAME option specifies a communication method that allows processes to communicate with one another without having to know where the sender and receiver processes are located. The name acts like an alias, connecting the two processes regardless of whether they are on the same computer or across connected domains.

Syntax

```
>>-NAMEDpipename--name-----------------------------------------><
```

Parameters

name
: Specifies the named pipes name for the server to use. Named pipes are ideal for running in an environment where client and server are on the same machine. No communication software is required and no setup is required.

Examples

```
namedpipename     \\.\PIPE\TSMPIPE
```

AIX | Linux | Windows

NDMPCONNECTIONTIMEOUT

The NDMPCONNECTIONTIMEOUT server option specifies the time in hours that IBM Spectrum Protect™ server waits to receive status updates during NDMP restore operations across the LAN. NDMP restore operations of large NAS file systems can have long periods of inactivity. The default is 6 hours.

Syntax

```
                          .-6-----.
>>-NDMPCONNECTIONTIMEOUT--+-hours-+---------------------------><
```

Parameters

hours
The number of hours that the IBM Spectrum Protect server waits to receive status updates during an NDMP restore operation over the LAN. The default value is 6. The minimum is 1 hour. The maximum is 48 hours.

Example

Specify a timeout of 10 hours before the NDMP connection times out:

```
ndmpconnectiontimeout  10
```

NDMPCONTROLPORT

The NDMPCONTROLPORT option specifies the port number to be used for internal communications for certain Network Data Management Protocol (NDMP) operations. The IBM Spectrum Protect™ server does not function as a general purpose NDMP tape server.

Syntax

```
                    .-10000-------.
>>-NDMPControlport--+-port_number-+---------------------------><
```

Parameters

port_number
The port number to be used for internal communications for certain NDMP operations. The port number must be from 1024 to 32767. The default is 10000.

Examples

```
ndmpcontrolport 9999
```

NDMPENABLEKEEPALIVE

The NDMPENABLEKEEPALIVE server option specifies whether the IBM Spectrum Protect™ server enables Transmission Control Protocol (TCP) keepalive on network data-management protocol (NDMP) control connections to network-attached storage (NAS) devices. The default is NO.

TCP keepalive is implemented within the network support of an operating system. TCP keepalive prevents a long-running, inactive connection from being closed by firewall software that detects and closes inactive connections.
Restriction: To prevent errors, do not enable TCP keepalive in certain types of environments. One example is environments that do not have firewalls between the IBM Spectrum Protect server and a NAS device. Another example is environments with firewalls that tolerate long-running, inactive connections. Enabling TCP keepalive in this type of environment can cause an idle connection to be inadvertently closed if the connection partner temporarily fails to respond to TCP keepalive packets.

Syntax

```
>>-NDMPENABLEKEEPALIVES--+-NO--+-------------------------------><
                         '-YES-'
```

Parameters

NO
Disable TCP keepalive on all NDMP control connections. NO is the default.
YES
Enable TCP keepalive on all NDMP control connections. The default idle time before the first TCP keepalive packet is sent is 120 minutes.

AIX | Linux | Windows To change the idle time, use the NDMPKEEPIDLEMINUTES server option.

Example

Enable TCP keepalive on all NDMP control connections so that inactive NDMP connections are not closed:

```
ndmpenablekeepalive yes
```

AIX | Linux | Windows

NDMPKEEPIDLEMINUTES

The NDMPKEEPIDLEMINUTES server option specifies the amount of time, in minutes, before the operating system transmits the first Transmission Control Protocol (TCP) keepalive packet on a network data-management protocol (NDMP) control connection. The default is 120 minutes.

Prerequisite: Use this option only after you set the value of the NDMPENABLEKEEPALIVES server option to YES.

Syntax

```
                          .-120-----.
>>-NDMPKEEPIDLEMINUTES--+-minutes-+---------------------------><
```

Parameters

minutes
: The number of minutes of inactivity on NDMP control connections before TCP keepalive packets are transmitted. The default value is 120. The minimum is 1 minute. The maximum is 600 minutes.

Example

Specify an idle time of 15 minutes before the first TCP keepalive packet is sent:

```
ndmpkeepidleminutes  15
```

NDMPPORTRANGE

The NDMPPORTRANGE option specifies the range of port numbers through which IBM Spectrum Protect™ cycles to obtain a port number for accepting a session from a network-attached storage (NAS) device for data transfer. The default is 0,0 which means that IBM Spectrum Protect lets the operating system provide a port (ephemeral port).

If all ports specified are in use when a NAS device attempts to connect to the server, the operation fails. If a single port number is chosen (no comma and no port number for the high value), the default for the high port number is the low port number plus 100.

When Network Data Management Protocol (NDMP) data is directed to an IBM Spectrum Protect native pool, communication can be initiated from either the NDMP systems or the IBM Spectrum Protect server. If a firewall separates the server and NAS devices, it may be necessary to specify port numbers in firewall rules to allow traffic to pass to and from the NAS devices. NAS devices communicate to the IBM Spectrum Protect server the port numbers that they will use when contacting the server. The port numbers of the server are controlled with the NDMPPortrange options. Port number control for NAS devices is specific to vendors. Consult your vendor documentation.

Syntax

```
>>-NDMPPortrange--port_number_low-+--------------------+--------><
                                  '-,port_number_high-'
```

Parameters

port_number_low
: The low port number from which IBM Spectrum Protect starts to cycle when needing a port number for accepting session from a NAS device for data transfer. The minimum port number value is 1024.

port_number_high
The high port number to which IBM Spectrum Protect can cycle when needing a port number for accepting session from a NAS device for data transfer. The maximum port number value is 32767. The high port number must be the same or larger than the low port number.

Examples

Specify that IBM Spectrum Protect can cycle from port numbers 1024 - 2024.

```
ndmpportrange 1024,2024
```

NDMPPREFDATAINTERFACE

This option specifies the IP address that is associated with the interface in which you want the server to receive all Network Data Management Protocol (NDMP) backup data.

This option affects all subsequent NDMP filer-to-server operations, but does not affect NDMP control connections, which use the system's default network interface. The value for this option is a host name or IPV4 address that is associated with one of the active network interfaces of the system on which the IBM Spectrum Protect™ server is running. This interface must be IPV4 enabled.

You can update this server option without stopping and restarting the server by using the SETOPT command.

Syntax

```
>>-NDMPPREFDATAINTERFACE--ip_address---------------------------><
```

Parameters

ip_address
Specify an address in either dotted decimal or host name format. If you specify a dotted decimal address, it is not verified with a domain name server. If the address is not correct, it can cause failures when the server attempts to open a socket at the start of an NDMP filer-to-server backup.

Host name format addresses are verified with a domain name server. There is no default value. If a value is not set, all NDMP operations use the IBM Spectrum Protect server's network interface for receiving backup data during NDMP filer-to-server backup operations.

To clear the option value, specify the SETOPT command with a null value, "".

Examples:

```
ndmpprefdatainterface  net1.tucson.ibm.com

ndmpprefdatainterface  9.11.152.89
```

NOPREEMPT

The server allows certain operations to preempt other operations for access to volumes and devices. You can specify the NOPREEMPT option to disable preemption. When preemption is disabled, no operation can preempt another for access to a volume, and only a database backup operation can preempt another operation for access to a device.

For example, a client data restore operation preempts a client data backup for use of a specific device or access to a specific volume.

Syntax

```
>>-NOPREEMPT---------------------------------------------------><
```

Parameters

None

Examples

Disable preemption among server operations:

```
nopreempt
```

NORETRIEVEDATE

The NORETRIEVEDATE option specifies that the server does not update the retrieve date of a file in a disk storage pool when a client restores or retrieves the file. This option and the MIGDELAY storage pool parameter control when the server migrates files.

If you do not specify NORETRIEVEDATE, the server migrates files after they have been in the storage pool for the number of days specified by the MIGDELAY parameter. The number of days is counted from the day that the file was stored in the storage pool or retrieved by a client, whichever is more recent. If you specify NORETRIEVEDATE, the server does not update the retrieve date of a file, and the number of days is counted from the day the file entered the disk storage pool.

If you specify this option and caching is enabled for a disk storage pool, reclamation of cached space is affected. When space is needed in a disk storage pool that contains cached files, the server gets the space by selectively erasing cached copies. Files that have the oldest retrieve dates and occupy the largest amount of space are selected for removal. When you specify NORETRIEVEDATE, the server does not update the retrieve date when a file is retrieved. This may cause cached copies to be removed even though they have recently been retrieved by a client.

Syntax

```
>>-NORETRIEVEDATE-------------------------------------------><
```

Parameters

None.

Examples

Specify that the retrieve dates of files in disk storage pools are not updated when clients restore and retrieve the files:

```
noretrievedate
```

Windows

NPAUDITFAILURE

The NPAUDITFAILURE option specifies whether an event is sent to the event log when a node logs in to the server using a name that is in the Windows group but does not match the Windows account login name. To ensure that a node can access only its own data, the node name and the Windows account name must match.

Syntax

```
>>-NPAUDITFailure--+-Yes-+-----------------------------------><
                   '-No--'
```

Parameters

Yes
: Specifies that an event is sent to the event log when a node logs in to the server using a name that is in the Windows group. But, this name does not match the Windows account login name.

No
Specifies that an audit failure event is not sent to the event log.

Examples

Specify that an event is sent to the event log when a node logs in to the server using a name that is in the Windows group. But, this name does not match the Windows account login name.

```
npauditfailure yes
```

Windows

NPAUDITSUCCESS

The NPAUDITSUCCESS option specifies that an event is sent to the event log when a client node user is authenticated for access to the server through SECUREPIPE.

Syntax

```
>>-NPAUDITSuccess--+-Yes-+-------------------------------------><
                   '-No--'
```

Parameters

Yes
Specifies that an event is sent to the event log when a client node user is authenticated for access to the server through SECUREPIPES.
No
Specifies that an event is not sent to the Windows log.

Examples

Specify that an event is sent to the event log when a client node is authenticated for access to the server.

```
npauditsuccess yes
```

Windows

NPBUFFERSIZE

The NPBUFFERSIZE option specifies the size of the Named Pipes communication buffer.

Syntax

```
                .-8---------.
>>-NPBUFfersize--+-kilobytes-+--------------------------------><
```

Parameters

kilobytes
Specifies the size, in kilobytes, of the Named Pipes communication buffer. The default is 8.

Examples

Specify a 16 KB Named Pipes communication buffer:

```
npbuffersize 16
```

Windows

NUMBERFORMAT

The NUMBERFORMAT option specifies the format in which the server displays numbers.

The value of NUMBERFORMAT is overridden by the number formatting definition of the locale if the locale is successfully initialized at server startup. The locale is specified in the LANGUAGE option.

Syntax

```
>>-NUMberformat--number----------------------------------------><
```

Parameters

number
: Select a number from 1 to 6 to identify the number format used by the server. The default is 1.

1
: 1,000.00

2
: 1,000,00

3
: 1 000,00

4
: 1 000.00

5
: 1.000,00

6
: 1'000,00

Examples

```
numberformat 4
```

NUMOPENVOLSALLOWED

The NUMOPENVOLSALLOWED option specifies the number of input FILE volumes in a deduplicated storage pool that can be open at one time.

Input volumes contain data to be read during client-restore operations and server processes, such as reclamation and migration. Use this option to improve performance by reducing the frequency with which volumes are opened and closed.

Each session within a client operation or server process can have as many open FILE volumes as specified by this option. A session is initiated by a client operation or by a server process. Multiple sessions can be started within each.

During a client restore operation, volumes can remain open for the duration of a client restore operation and as long a client session is active. During a no-query restore operation, the volumes remain open until the no-query restore completes. At that time, all volumes are closed and released. However, for a classic restore operation started in interactive mode, the volumes might remain open at the end of the restore operation. The volumes are closed and released when the next classic restore operation is requested.

Set this value in the server options file or use the SETOPT command.

Tip: This option can significantly increase the number of volumes and mount points in use at any one time. To optimize performance, follow these steps:

- To set NUMOPENVOLSALLOWED, select a beginning value (the default is recommended). Monitor client sessions and server processes. Note the highest number of volumes open for a single session or process. Increase the setting of NUMOPENVOLSALLOWED if the highest number of open volumes is equal to the value specified by NUMOPENVOLSALLOWED.
- To prevent sessions or processes from having to wait for a mount point, increase the value of the MOUNTLIMIT parameter in the device-class definition. Set the value of the MOUNTLIMIT parameter high enough to allow all client sessions and

server processes using deduplicated storage pools to open the number of volume specified by the NUMOPENVOLSALLOWED option. For client sessions, check the destination in the copy group definition to determine how many nodes are storing data in the deduplicated storage pool. For server processes, check the number of processes allowed for each process for the storage pool.

- A situation might occur in which a node backs up and restores or archives and retrieves concurrently to and from a deduplicated storage pool. All the mount points required for these operations increase the total number of mount points required by the node.

  As a result, the node might not be able to start additional backup sessions if it already has more mount points open than what the MAXNUMMP parameter in the client-node definition allows. This can occur even though the MOUNTLIMIT for the device class was not exceeded.

  To prevent backup and retrieve operations from failing, set the value of the MAXNUMMP parameter in the client-node definition to a value at least as high as the NUMOPENVOLSALLOWED option. Increase this value if you notice that the node is failing backup or retrieve operations because the MAXNUMMP value is being exceeded.

Syntax

```
>>-NUMOPENVOLSallowed--number_of_open_volumes------------------><
```

Parameters

number_of_open_volumes
: Specifies the number of input FILE volumes in a deduplicated storage pool that can be open at one time. The default is 10. The minimum value is 3. The maximum value is 999.

Examples

Specify that up to 5 volumes in a deduplicated storage pool can be open at one time.

```
numopenvolsallowed 5
```

AIX | Linux | Windows

PUSHSTATUS

The PUSHSTATUS option is used on spoke servers to ensure that status information is sent to the hub server. Do not update this option unless you must restore the Operations Center configuration to the preconfigured state where the IBM Spectrum Protect™ servers are not defined as hub or spoke servers.

If you must restore the Operations Center configuration to the preconfigured state, you must issue the following command on each spoke server:

```
SETOPT PUSHSTATUS NO
```

QUERYAUTH

The QUERYAUTH option specifies the administrative authority level required to issue QUERY or SQL SELECT commands. By default any administrator can issue QUERY and SELECT commands. You can use this option to restrict the use of these commands.

Syntax

```
>>-QUERYAuth--+-NOne-----+-------------------------------------><
              +-SYstem---+
              +-POlicy---+
              +-STorage--+
              '-OPerator-'
```

Parameters

NOne
: Any administrator can issue QUERY or SELECT commands without requiring any administrative authority.

SYstem
: Administrators must have SYSTEM authority to issue QUERY or SELECT commands.

POlicy
: Administrators must have POLICY authority over one or more policy domains or SYSTEM authority to issue QUERY or SELECT commands.

STorage
: Administrators must have STORAGE authority over one or more storage pools or SYSTEM authority to issue QUERY or SELECT commands.

OPerator
: Administrators must have OPERATOR or SYSTEM authority to issue QUERY or SELECT commands.

Examples

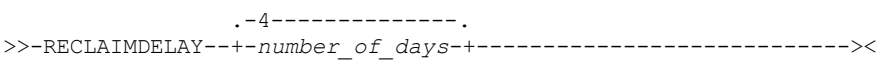
To restrict the use of QUERY and SELECT commands to administrators with system or storage authority, enter:

```
queryauth storage
```

RECLAIMDELAY

This option delays the reclamation of a SnapLock volume, allowing remaining data to expire so that there is no need to reclaim the volume.

Syntax



Parameters

number_of_days
: Specifies the number of days to delay the reclamation of a SnapLock volume.
Before a SnapLock volume is reclaimed, the IBM Spectrum Protect™ server allows the specified number of days to pass, so that any files remaining on the volume have a chance to expire. The default reclaim delay period is 4 days and can be set anywhere from 1 to 120 days.

Examples

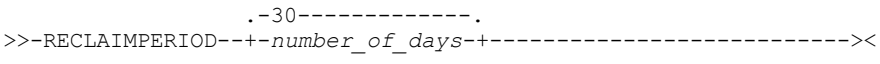
Specify that the number of days to delay reclamation is 30 days:

```
reclaimdelay 30
```

RECLAIMPERIOD

This option allows you to set the number of days for the reclamation period of a SnapLock volume.

Syntax



Parameters

number_of_days
: Specifies the number of days that are allowed for the reclamation period of a SnapLock volume.
After the retention of a SnapLock volume has expired, the IBM Spectrum Protect™ server will reclaim the volume within the specified number of days if there is still data remaining on the volume. The default reclaim period is 30 days and can be set

anywhere from 7 to 365 days.

The reclamation period does not begin until the RECLAIMDELAY period has expired.

Examples

Specify that the reclaim period is 45 days:

```
reclaimperiod 45
```

REORGBEGINTIME

The REORGBEGINTIME option specifies the earliest time that the IBM Spectrum Protect™ server can start a table or index reorganization.

Schedule server-initiated reorganizations to start during periods when server activity is low. Use this option together with the REORGDURATION option. The REORGDURATION specifies an interval during which reorganization can start.

Syntax

```
>>-REORGBEGINTime--hh:mm----------------------------------------><
```

Parameters

hh:mm

Specifies the time that the server can start a reorganization: The default start time 6:00 a.m. Use a 24-hour format to specify the time.

Time	Description	Values
hh	The hour of the day	Specify a number 00 - 23.
mm	The minute of the hour	Specify a number 00 - 59.

Examples

Specify 6:00 a.m. as the earliest time that a reorganization can start.

```
reorgbegintime 06:00
```

Specify 8:30 p.m. as the earliest time that a reorganization can start.

```
reorgbegintime 20:30
```

Specify noon as the earliest time that a reorganization can start.

```
reorgbegintime 12:00
```

Specify 3:30 p.m. as the earliest time that a reorganization can start.

```
reorgbegintime 15:30
```

Specify midnight as the earliest time that a reorganization can start.

```
reorgbegintime 00:00
```

REORGDURATION

The REORGDURATION option specifies an interval during which server-initiated table or index reorganization can start.

Schedule server-initiated reorganizations to start during periods when server activity is low. Use this option together with the REORGBEGINTIME option. The REORGBEGINTIME option specifies the earliest time that the server can start a reorganization.

Syntax

```
>>-REORGDURation--nn-----------------------------------------><
```

Parameters

nn
: Specifies the number of hours during which a reorganization can start. The minimum value is 1, the maximum value is 24. The default value is 24.

Example

Specify an interval of four hours during which a reorganization can start.

```
reorgduration 4
```

REPORTRETRIEVE

The REPORTRETRIEVE option reports on restore or retrieve operations that are performed by client nodes or administrators. The default is NO.

Syntax

```
>>-REPORTRETRIEVE--+-YES-+-------------------------------------><
                   '-NO--'
```

Parameters

YES
: Specifies that messages will be issued to the server console and stored in the activity log whenever files are restored or retrieved from the IBM Spectrum Protect™ server. The messages will specify the name of the objects being restored or retrieved and identify the client node or administrator performing the operation.

NO
: Specifies that messages will not be issued.

Examples

Specify that messages will be issued and stored in the activity log whenever files are restored or retrieved from the IBM Spectrum Protect server:

```
reportretrieve yes
```

The following message is issued for an administrator client session:

```
ANR0411I Session 8 for administrator COLIND-TUC logged in as node
COLIND-TUC restored or retrieved Backup object: node COLIND-TUC,
filespace \\colind-tuc\c$, object\CODE\TESTDATA\ XXX.OUT
```

REPLBATCHSIZE

The REPLBATCHSIZE option specifies the number of client files that are to be replicated in a batch, within the same server transaction. This option affects only the node replication processes and works with the REPLSIZETHRESH option to improve node replication processing.

The REPLBATCHSIZE option limits the number of files in a transaction and the REPLSIZETHRESH option limits the number of bytes in a transaction. The transaction ends when either the REPLBATCHSIZE threshold or the REPLSIZETHRESH threshold is reached.

Syntax

```
                  .-4096-----------.
>>-REPLBatchsize--+-number_of_files-+-------------------------><
```

Parameters

number_of_files
: Specifies a number of files between 1 - 32768. The default is 4096.

Examples

```
replbatchsize 25000
```

REPLSIZETHRESH

The REPLSIZETHRESH option specifies, in megabytes, a threshold for the amount of data replicated, within the same server transaction.

The amount of data is based on the non-deduplicated size of the file, which is the original size of the file. The amount of data that is replicated is controlled by the threshold. When the amount of data exceeds the threshold, the server ends the transaction and no more files are added to the current batch. A new transaction is started after the current batch is replicated. This option is used with the REPLBATCHSIZE option.

For example, suppose that a file is 10 MB and is stored in a data-deduplication-enabled storage pool and only 2 MB of the file is transferred during replication. The amount of data replicated includes the 10 MB size of the file, and excludes the 2 MB transferred. When the amount of data replicated exceeds the value specified for the REPLSIZETHRESH threshold, the transaction ends.

Tip: If you are replicating data from a source server in the cloud and frequently get an ANR1880W server message on the target server, lower the value of the REPLSIZETHRESH option on the source server.

Syntax

```
                  .-4096------.
>>-REPLSizethresh--+-megabytes-+-----------------------------><
```

Parameters

megabytes
: Specifies the number of megabytes as an integer from 1 - 32768. The default value is 4096.

Examples

```
replsizethresh 2000
```

REQSYSAUTHOUTFILE

The REQSYSAUTHOUTFILE option specifies if system authority is required for administrative commands that cause IBM Spectrum Protect™ to write to an external file.

This option applies to the following commands:

- BACKUP DEVCONFIG with the FILENAMES parameter
- BACKUP VOLHISTORY with the FILENAMES parameter
- DEFINE BACKUPSET
- DELETE BACKUPSET
- GENERATE BACKUPSET
- MOVE DRMEDIA with the CMD parameter
- MOVE MEDIA with the CMD parameter
- QUERY DRMEDIA with the CMD parameter

- QUERY MEDIA with the CMD parameter
- QUERY SCRIPT with the OUTPUTFILE parameter

Syntax

```
>>-REQSYSauthoutfile--+-Yes-+---------------------------------><
                      '-No--'
```

Parameters

Yes
: System authority is required for administrative commands that cause IBM Spectrum Protect to write to an external file.

No
: System authority is not required for administrative commands that cause IBM Spectrum Protect to write to an external file. That is, there is no change to the authority level that is required to issue the command.

Examples

```
reqsysauthoutfile no
```

RESOURCETIMEOUT

The RESOURCETIMEOUT option specifies how long the server waits for a resource before canceling the pending acquisition of a resource. When a timeout occurs the request for the resource will be canceled.

Note: When managing a set of shared library resources, such as servers designated as library managers and clients, consider setting this option at the same time limit for all participants in the shared configuration. In any case of error recovery, IBM Spectrum Protect™ will always defer to the longest time limit.

Syntax

```
                    .-60------.
>>-RESOURCETimeout--+-minutes-+--------------------------------><
```

Parameters

minutes
: Specifies the maximum number of minutes that the server waits for a resource. The default value is 60 minutes. The minimum value is 1 minute.

Examples

Specify that the server will wait 15 minutes for a server resource:

```
resourcetimeout 15
```

RESTHTTPSPORT

The RESTHTTPSPORT option specifies the port number to be used for Hypertext Transfer Protocol Secure (HTTPS) communication between the Operations Center and the hub server.

Syntax

```
                  .-8443--------.
>>-RESTHTTPSport--+-secure_port-+-----------------------------><
```

Parameters

secure_port
: Specifies the port number that is used for secure communications between the hub server and the Operations Center. The range of values is 1025 - 32767; the default is 8443.

Example

Specify that port number 8444 is used for HTTPS communication.

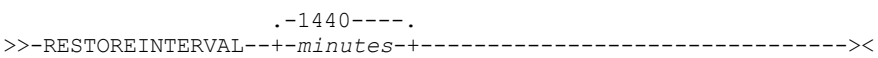
```
restHttpsPort 8444
```

RESTOREINTERVAL

The RESTOREINTERVAL option specifies how long a restartable restore session can be saved in the server database. As long as the restore session is saved in the database, it can be restarted from the point at which it stopped.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax



Parameters

minutes
: Specifies how long, in minutes, that a restartable restore session can be in the database before it can be expired. The minimum value is 0. The maximum is 10080 (one week). The default is 1440 minutes (24 hours). If the value is set to 0 and the restore is interrupted or fails, the restore is still put in the restartable state. However, it is immediately eligible to be expired.

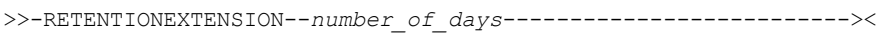
Examples

```
restoreinterval 1440
```

RETENTIONEXTENSION

The RETENTIONEXTENSION option specifies the number of days to extend the retention date of a SnapLock volume. This option allows the server to extend the retention date of a SnapLock volume in order to avoid excessive reclamation.

Syntax



Parameters

number_of_days
: Specifies the number of days to extend the retention date of a SnapLock volume. The minimum value is 30 days; the maximum value is 9999 days; the default is 365.
If you specify a value of 0 (zero) for the RETVER parameter of an archive copy group, the actual value that is used for RETVER is the value of the option RETENTIONEXTENSION, if one of the following conditions is also true:

  - The destination storage pool for the archive copy group is a SnapLock storage pool.
  - The storage pool that is the target for a storage pool migration or of a MOVE DATA or MOVE NODEDATA command is a SnapLock storage pool.

If a SnapLock volume is the target volume for data from another SnapLock volume and if the remaining retention of the data on the volume is less than the value specified, then the retention date is set using the value specified. Otherwise, the remaining retention of the data is used to set the retention of the volume.
If a SnapLock volume has entered the reclamation period but the percentage of reclaimable space of the volume has not exceeded the reclamation threshold of the storage pool or the value specified on the THRESHOLD parameter of a RECLAIM STGPOOL command, then the retention date of the SnapLock volume is extended by the amount specified in the RETENTIONEXTENSION option.

Examples

Specify that the retention date is extended by 60 days:

```
retentionextension 60
```

AIX | Linux | Windows

SANDISCOVERY

The SANDISCOVERY option specifies whether the IBM Spectrum Protect™ SAN discovery function is enabled.

To use SAN discovery, all devices on the SAN must have a unique device serial number. When set to ON, the server completes SAN discovery in the following instances:

- When the device path is changed
- When the QUERY SAN command is issued

Using SAN discovery, the server can automatically correct the special file name for a device if it is changed for a specified tape device.

The IBM Spectrum Protect server does not require persistent binding with the SAN discovery function enabled. To display a list of devices that are seen by the server, you can issue the QUERY SAN command.

Syntax

```
   .-SANDISCOVERY--=--OFF-----------------.
>>-+-------------------------------------+------------------><
   '-SANDISCOVERY--=--+-ON---------------+-'
                      '-UNSCANNEDPATHOFF-'
```

Parameters

ON
: Specifies that the server completes SAN discovery when the device path is changed, or when the QUERY SAN command is issued.

OFF
: Specifies that the server does not complete SAN discovery when the device path is changed, or when the QUERY SAN command is issued. If the IBM Spectrum Protect server is not able to open a device, a message is issued but the path that is associated with the device is not taken offline. This value is the default.

UNSCANNEDPATHOFF
: Specifies that the server does not complete SAN discovery when the device path is changed, or when the QUERY SAN command is issued. If the IBM Spectrum Protect server is not able to open a device, a message is issued and the path to the device is taken offline.

Examples

```
sandiscovery on
```

Related commands

Table 1. Commands related to SANDISCOVERY

Command	Description

Command	Description
PERFORM LIBACTION	Defines all drives and paths for a library.

AIX Linux Windows

SANDISCOVERYTIMEOUT

The SANDISCOVERYTIMEOUT option specifies the amount of time allowed for host bus adapters to respond when they are queried by the SAN discovery process. Once the time specified for the SANDISCOVERYTIMEOUT is reached, the process times out.

Syntax

```
>>-SANDISCOVERYTIMEOUT--value---------------------------------><
```

Parameters

value
: Specifies the amount of time to elapse before the SAN discovery process times out. The range is from 15 to 1800 seconds. The default is 15 seconds.

Examples

```
sandiscoverytimeout 45
```

AIX Linux Windows

SANREFRESHTIME

The SANREFRESHTIME option specifies the amount of time that elapses before the cached SAN discovery information is refreshed. The SANREFRESHTIME option has a default value of 0, which means that there is no SAN discovery cache. The information is obtained directly from the host bus adapter (HBA) every time the server performs a SAN discovery operation.

Note: The QUERY SAN server command always receives SAN information at the time that the command is issued and ignores any value specified for SANREFRESHTIME.

Syntax

```
                    .-0----.
>>-SANREFRESHTIME--+-time-+-----------------------------------><
```

Parameters

time
: The length of time, in seconds, before the cached SAN discovery information is refreshed. The default value is 0 and specifies that SAN discovery information is not cached. If a value other than 0 is specified, for example, 100 seconds, then the SAN discovery information is refreshed 100 seconds after the prior SAN discovery operation.

Examples

Refresh SAN discovery information after 100 seconds.

```
sanrefreshtime 100
```

Turn off the caching of SAN discovery information.

```
sanrefreshtime 0
```

SEARCHMPQUEUE

The SEARCHMPQUEUE option specifies the order in which the server satisfies requests in the mount queue. If the option is specified, the server first tries to satisfy requests for volumes that are already mounted. These requests may be satisfied before other requests, even if the others have been waiting longer for the mount point. If this option is not specified, the server satisfies requests in the order in which they are received.

Syntax

```
>>-SEARCHMPQUEUE-----------------------------------------------><
```

Parameters

None

Examples

Specify that the server tries to first satisfy a request for a volume that is already mounted:

```
searchmpqueue
```

Windows

SECUREPIPES

When using the named pipes protocol, enabling SECUREPIPES forces the server to check the Windows group designated by ADSMGROUPNAME in order to authenticate a client node/user.

The user name and password defined in the Windows group are used to authenticate the node/user for access to the server data. The node/user must also be a registered IBM Spectrum Protect™ client node. However, the IBM Spectrum Protect client node password is ignored, and the Windows password associated with the user is used.

Syntax

```
>>-SECUREPipes--+-Yes-+---------------------------------------><
                '-No--'
```

Parameters

Yes
: Specifies that IBM Spectrum Protect checks the Windows group designated by ADSMGROUPNAME in order to authenticate a client node/user.

No
: Specifies that IBM Spectrum Protect does not check the Windows group designated by ADSMGROUPNAME in order to authenticate a client node/user.

Examples

Specify that IBM Spectrum Protect checks the Windows group to authenticate client nodes.

```
securepipes yes
```

SERVERDEDUPTXNLIMIT

The SERVERDEDUPTXNLIMIT option specifies the maximum size of objects that can be deduplicated on the server.

When you use duplicate-identification processes (the IDENTIFY DUPLICATES command) for large objects, intensive database activity can result from long-running transactions that are required to update the database. High levels of database activity can

produce following symptoms:

- Reduced throughput for client backup and archive operations
- Resource contention resulting from concurrent server operations
- Excessive recovery log activity

The extent to which these symptoms occur depends on the number and size of objects being processed, the intensity and type of concurrent operations taking place on the IBM Spectrum Protect™ server, and the IBM Spectrum Protect server configuration.

With the SERVERDEDUPTXNLIMIT server option, you can specify a maximum size, in gigabytes, for objects that can be deduplicated on the server. If an object or set of objects in a single transaction exceeds the limit specified by SERVERDEDUPTXNLIMIT, the objects are not deduplicated by the server. You can specify a value 32 - 102400 GB. The default value is 5120 GB.

Increasing the value of this option causes the IBM Spectrum Protect server to search for objects previously deferred whose size falls below the new transaction limit.

Remember: The search for objects previously deferred can take time. Use care when increasing the value of SERVERDEDUPTXNLIMIT. Reducing the value of this option does not cause IBM Spectrum Protect to search for deferred objects.

The appropriate value for this option depends on the IBM Spectrum Protect server configuration and concurrent server activity. You can specify a high value for this option if you minimize resource contention. To minimize resource contention, perform operations, such as backup, archive, duplicate identification, and reclamation, at different times.

To update this server option without stopping and restarting the server, use the SETOPT command.

Syntax

```
                        .-5120------.
>>-SERVERDEDUPTXNlimit--+-gigabytes-+-------------------------><
```

Parameters

gigabytes
: Specifies the maximum size, in gigabytes, of objects that can be duplicated on the server. You can specify a value 32 - 102400. The default value is 5120.

Examples

Disable server-side deduplication for all objects over 120 GB:

```
serverdeduptxnlimit 120
```

SHMPORT

AIX Linux The SHMPORT option specifies the TCP/IP port address of a server when using shared memory. All shared memory communications start with a TCP/IP connection. Windows The SHMPORT option specifies the port that the server listens on for shared memory connections.

Syntax

```
>>-SHMPort--port_number-----------------------------------------><
```

Parameters

port_number
: Specifies the port number. AIX Linux You can specify a value from 1024 to 32767. The default value is 1510. Windows You can specify a value from 1 to 32767. The default value is 1.

Examples

AIX | Linux

```
shmport  1580
```

Windows

```
shmport  1
```

SHREDDING

The SHREDDING option specifies whether shredding of deleted sensitive data is performed automatically or manually. Shredding applies only to data in storage pools that have been explicitly configured to support shredding.

Syntax

```
>>-SHREDding--+-AUTOmatic-+-------------------------------------><
              '-MANual----'
```

Parameters

AUTOmatic
: Specifies that shredding occurs automatically as sensitive data is deleted. Use this option to shred sensitive data as soon as possible after it is deleted. If the SHREDDING option is not specified, this is the default behavior. If there is an I/O error during automatic shredding, an error is reported, and shredding of the current object halts. If the I/O error cannot be corrected, you might need to run shredding manually and use the IOERROR keyword.

MANual
: Specifies that shredding occurs manually, only when the SHRED DATA command is invoked. Use this option to control when shredding takes place, in order to ensure that it does not interfere with other server activities.
Tip: If you specify manual shredding, run the SHRED DATA command regularly, at least as often as you perform other routine server-maintenance tasks (for example, expiration, reclamation, and so on). Doing so can prevent performance degradation of certain server processes (in particular, migration). For best results, run SHRED DATA after any operation (for example, expiration and migration) that deletes files from a shred pool.

Examples

Specify that IBM Spectrum Protect™ automatically shreds data in a storage pool configured for shredding after that data is deleted:

```
shredding automatic
```

SNMPHEARTBEATINTERVAL

The SNMPHEARTBEATINTERVAL option specifies the interval in minutes between queries of the IBM Spectrum Protect™ server.

Syntax

```
                          .-5-------.
>>-SNMPHEARTBEATINTERVAL--+-minutes-+-------------------------><
```

Parameters

minutes
: Specifies the heartbeat interval in minutes. Valid values are from 0 to 1440 (one day). The default is 5 minutes.

Examples

```
snmpheartbeatinterval 20
```

SNMPMESSAGECATEGORY

The SNMPMESSAGECATEGORY option specifies the trap types used when messages are forwarded from the server, through the Simple Network Management Protocol (SNMP) subagent, to the SNMP manager.

Syntax

```
>>-SNMPMESSAGECATEGORY--+-SEVERITY---+------------------------><
                        '-INDIVIDUAL-'
```

Parameters

SEVERITY
: Specifies that there are four trap types based on message severity level:

  1
  : Severe

  2
  : Error

  3
  : Warning

  4
  : Information

  This is the default.

INDIVIDUAL
: Specifies that a separate trap type is used for each message. The numeric part of the message identifier indicates the trap type.

Examples

```
snmpmessagecategory individual
```

SNMPSUBAGENT

The SNMPSUBAGENT option specifies the parameters needed for the IBM Spectrum Protect™ subagent to communicate with the Simple Network Management Protocol (SNMP) daemon. This option is only to configure the SNMP subagent for communicating with the SNMP agent; it is ignored by the server.

Syntax

```
>>-SNMPSUBAGENT--+---------------------+------------------------>
                 '-HOSTname--host_name-'

>--+-------------------------------+--+------------------+-----><
   '-COMMunityname--community_name-'  '-TIMEOUT--seconds-'
```

Parameters

HOSTname host_name
: Specifies the TCP/IP name or number of the host running the SNMP agent that the IBM Spectrum Protect SNMP subagent connects to. This parameter is optional. The default name is *localhost*.

COMMunityname community_name
: Specifies the configured community name on the system running the SNMP agent. This parameter is optional. The default name is *public*.

TIMEOUT seconds
: Specifies the time, in seconds, in which a request must be received. This parameter is optional. The default value is 600.

Examples

```
snmpsubagent hostname jimbo communityname public timeout 2600
```

SNMPSUBAGENTHOST

The SNMPSUBAGENTHOST option specifies the location of the IBM Spectrum Protect™ Simple Network Management Protocol (SNMP) subagent. The default for this option is 127.0.0.1.

Syntax

```
>>-SNMPSUBAGENTHOST--host_name---------------------------------><
```

Parameters

host_name
: Specifies the TCP/IP host name or number on which the IBM Spectrum Protect SNMP subagent is located. The subagent and server must be on the same node.

Examples

```
snmpsubagenthost 9.116.23.450
```

SNMPSUBAGENTPORT

The SNMPSUBAGENTPORT option specifies the port number of the IBM Spectrum Protect™ Simple Network Management Protocol (SNMP) subagent.

Syntax

```
>>-SNMPSUBAGENTPORT--port_number------------------------------><
```

Parameters

port_number
: Specifies the port number of the IBM Spectrum Protect SNMP subagent. Valid values are 1000 - 32767. The default is 1521.

Examples

```
snmpsubagentport 1525
```

SSLFIPSMODE

The SSLFIPSMODE option specifies whether the Federal Information Processing Standards (FIPS) mode is in effect for Secure Sockets Layer (SSL). The default is NO.

Because SSLv3 is not supported by FIPS mode, when you are using SSL with Version 6.1 or V5.5 clients, you must turn off FIPS mode.

Syntax

```
   .-SSLFIPSMODE--==--No------.
>>-+------------------------+-------------------------------><
   '-SSLFIPSMODE--==--+-No--+-'
                      '-Yes-'
```

Parameters

No
: Specifies that SSL FIPS mode is not active on the server. This setting is required when Backup-Archive Client versions previous to IBM Spectrum Protect™ 6.3 are to connect to the server with SSL.

Yes
: A value of YES indicates that SSL FIPS mode is active on the server. This setting restricts SSL session negotiation to use FIPS-approved cipher suites. Specifying YES is suggested when SSL communication is activated and all Backup-Archive Clients are at V6.3 or later.

Example: Enable SSL FIPS mode on the server

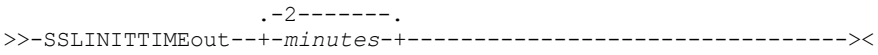
```
sslfipsmode yes
```

SSLINITTIMEOUT

The SSLINITTIMEOUT option specifies the time, in minutes, that the server waits for a Secure Sockets Layer (SSL) session to complete initialization before the server cancels the session.

When you specify this option, an SSL session is canceled if a client, server, or storage agent is not configured for SSL and tries to start an SSL session. Similarly, an SSL session is canceled if a client SSL session and a server are not configured with the same Transport Layer Security (TLS) version. In these situations, the SSL session might fail to completely initialize. The server cancels the session when the specified timeout is reached.

Syntax



Parameters

minutes
: Specifies the maximum number of minutes that a server waits for an SSL session to complete initialization. The default value is 2 minutes. The minimum value is 1 minute.

Example

```
sslinittimeout 1
```

SSLTCPADMINPORT

The SSLTCPADMINPORT option specifies the port address on which the server TCP/IP communication driver waits for requests for SSL-enabled sessions only. The sessions are for the command-line administrative client.

Note: Beginning with IBM Spectrum Protect™ Version 8.1.2 and Tivoli® Storage Manager Version 7.1.8, you are no longer required to use the SSLTCPPORT or SSLTCPADMINPORT option to allow SSL-enabled sessions from the client. The port number that is specified in the TCPPORT or TCPADMINPORT option listens for both TCP/IP and SSL-enabled client sessions.
The following types of sessions do not use the Secure Sockets Layer (SSL) protocol:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Database restore operations

If the ADMINONCLIENTPORT option is set to NO, SSL-enabled sessions for the administrative client require that different port numbers are set for the SSLTCPADMINPORT and SSLTCPPORT options.
Restrictions:

The following restrictions apply when you specify the SSL-only server ports (SSLTCPPORT and SSLTCPADMINPORT):

- When you specify the server's SSL-only port for the LLADDRESS on the DEFINE SERVER or UPDATE SERVER command, you must also specify the SSL=YES parameter.
- When you specify the server's SSL-only port for the client's TCPPORT option, you must also specify YES for the SSL client option.

The TCP/IP communications driver must be enabled with COMMMETHOD TCPIP or COMMMETHOD V6TCPIP.

Syntax

```
>>-SSLTCPADMINPort--port_number------------------------------><
```

Parameters

port_number
: Specifies the port number of the server. Valid values are 1024 - 32767. There is no default.

Examples

```
ssltcpadminport 1543
```

SSLTCPPORT

The SSLTCPPORT option specifies the Secure Sockets Layer (SSL) port number for SSL-enabled sessions only. The server TCP/IP communication driver waits for requests on this port for SSL-enabled sessions from the client.

Important: Beginning with IBM Spectrum Protect™ Version 8.1.2 and Tivoli® Storage Manager Version 7.1.8, you are no longer required to use the SSLTCPPORT or SSLTCPADMINPORT option to allow SSL-enabled sessions from the client. The port number that is specified in the TCPPORT or TCPADMINPORT option listens for both TCP/IP and SSL-enabled client sessions.
The following types of sessions do not use SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Database restore operations

If the ADMINONCLIENTPORT option is set to NO, SSL-enabled sessions for the administrative client require that different port numbers are specified for the SSLTCPADMINPORT and SSLTCPPORT options.

If you specify the same port number for the SSLTCPPORT and TCPPORT options, only SSL connections are accepted and TCP/IP connections are disabled for the port.
Restrictions:
The following restrictions apply when you specify the SSL-only server ports (SSLTCPPORT and SSLTCPADMINPORT):

- When you specify the server's SSL-only port for the LLADDRESS on the DEFINE SERVER or UPDATE SERVER command, you must also specify the SSL=YES parameter.
- When you specify the server's SSL-only port for the client's TCPPORT option, you must also specify YES for the SSL client option.

The TCP/IP communications driver must be enabled with COMMMETHOD TCPIP or COMMMETHOD V6TCPIP.

Syntax

```
>>-SSLTCPPort--port_number-------------------------------------><
```

Parameters

port_number
: Specifies the port number of the server. Valid values are 1024 - 32767. There is no default.

Examples

```
ssltcpport 1542
```

TCPADMINPORT

The TCPADMINPORT option specifies the port number on which the server TCP/IP communication driver waits for requests for TCP/IP and SSL-enabled sessions other than client sessions. This includes administrative sessions, server-to-server sessions, storage agent sessions, library client sessions, managed server sessions, and event server sessions.

Using different port numbers for the options TCPPORT and TCPADMINPORT enables you to create one set of firewall rules for client sessions and another set for the previously listed session types. By using the SESSIONINITIATION parameter of REGISTER NODE and UPDATE NODE commands, you can close the port specified by TCPPORT at the firewall, and specify nodes whose scheduled sessions will be started from the server. If the two port numbers are different, separate threads are used to service client sessions and the session types. If you allow the two options to use the same port number (by default or by explicitly setting them to the same port number), a single server thread is used to service all session requests.

Client sessions attempting to use the port specified by TCPADMINPORT are terminated (if TCPPORT and TCPADMINPORT specify different ports). Administrative sessions are allowed on either port, (unless the ADMINONCLIENTPORT option is set to NO) but by default administrative sessions use the port that is specified by TCPADMINPORT.

SSL-enabled sessions that use the TCPADMINPORT option have the same limitations as the SSLTCPADMINPORT option. The following types of sessions do not use the Secure Sockets Layer (SSL) protocol:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Database restore operations

If the ADMINONCLIENTPORT option is set to NO, SSL-enabled sessions for the administrative client require that different port numbers are specified for the TCPADMINPORT andTCPPORT options.

Syntax

```
>>-TCPADMINPort--port_number-----------------------------------><
```

Parameters

port_number
: Specifies the port number of the server. Valid values are 1024 - 32767. The default is the value of TCPPORT.

Examples

```
tcpadminport 1502
```

AIX | Linux

TCPBUFSIZE

The TCPBUFSIZE option specifies the size of the buffer used for TCP/IP send requests. During a restore, client data moves from the IBM Spectrum Protect™ session component to a TCP communication driver. The TCPBUFSIZE option determines if the server sends the data directly from the session buffer or copies the data to the TCP buffer. A 32 KB buffer size forces the server to copy data to its communication buffer and flush the buffer when it fills.

Note: This option is not related to the TCPWINDOWSIZE option.

Syntax

```
>>-TCPBufsize--kilobytes---------------------------------------><
```

Parameters

kilobytes
: Specifies the size, in kilobytes, of the buffer used for TCP/IP send requests.

  AIX The value range is from 1 to 64. The default is 32.

  Linux The value range is from 1 to 64. The default is 16.

Examples

```
tcpbufsize 5
```

TCPNODELAY

The TCPNODELAY option specifies whether the server disables the delay of sending successive small packets on the network.

Change the value from the default of YES only under one of these conditions:

- You are directed to change the option by your service representative.
- You fully understand the effects of the TCP Nagle algorithm on network transmissions. Setting the option to NO enables the Nagle algorithm, which delays sending small successive packets.

Syntax

```
>>-TCPNodelay--+-Yes-+-----------------------------------------><
               '-No--'
```

Parameters

Yes
: Specifies that the server allows successive small packets to be sent immediately over the network. Setting this option to YES might improve performance in some high-speed networks. The default is YES.

No
: Specifies that the server does not allow successive small packets to be sent immediately over the network.

Examples

```
tcpnodelay no
```

TCPPORT

The TCPPORT option specifies the port number on which the server TCP/IP communication driver waits for requests for client sessions. The server TCP/IP communication driver listens on this port for both TCP/IP and SSL-enabled sessions from the client.

Using different port numbers for the options TCPPORT and TCPADMINPORT enables you to create one set of firewall rules for client sessions and another set for other session types (administrative sessions, server-to-server sessions, storage agent sessions, library client sessions, managed server sessions, and event server sessions). If the two port numbers are different, separate threads are used to service client sessions and the other session types. If you allow the two options to use the same port number (by default or by explicitly setting them to the same port number), a single server thread is used to service all session requests.

SSL-enabled client sessions that use the TCPPORT option have the same limitations as the SSLTCPPORT option. The following types of sessions do not use SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Database restore operations

If the ADMINONCLIENTPORT option is set to NO, SSL-enabled sessions for the administrative client require that different port numbers are specified for the TCPADMINPORT and TCPPORT options.
If you specify the same port number for both the SSLTCPPORT and TCPPORT options, only SSL connections are accepted and TCP/IP connections are disabled for the port.

Windows You can change this option with the SETOPT command. When you change a port, the IBM Spectrum Protect™ server starts listening on the new port immediately. All current connections remain in use until closed.

Syntax

```
>>-TCPPort--port_number---------------------------------------><
```

Parameters

port_number
Specifies the port number of the server. Valid values are 1024 - 32767. The default value is 1500.

```
tcpport 1500
```

TCPWINDOWSIZE

The TCPWINDOWSIZE option specifies, in kilobytes, the amount of receive data that can be buffered at one time on a TCP/IP connection. The sending host cannot send more data until it receives an acknowledgment and a TCP receive window update. Each TCP packet contains the advertised TCP receive window on the connection. A larger window lets the sender continue sending data, and may improve communication performance, especially on fast networks with high latency.

Note:

- To improve backup performance, increase the TCPWINDOWSIZE on the server. To improve restore performance, increase the TCPWINDOWSIZE on the client.
- The TCP window acts as a buffer on the network.
- A window size larger than the buffer space on the network adapter might degrade throughput due to resending packets that were lost on the adapter.
- AIX Linux The TCPWINDOWSIZE option is not related to the TCPBUFFSIZE option nor to the send and receive buffers allocated in client or server memory.

Syntax

```
>>-TCPWindowsize--kilobytes-----------------------------------><
```

Parameters

kilobytes

Specifies the size you want to use, in kilobytes, for the TCP/IP sliding window for your client node. You can specify a value from 0 to 2048. The default is 63. If you specify 0, the server uses the default window size set by the operating system. Values from 1 to 2048 indicate that the window size is in the range of 1 KB to 2 MB.

Examples

```
tcpwindowsize 63
```

TECBEGINEVENTLOGGING

The TECBEGINEVENTLOGGING option specifies whether event logging for the Tivoli® receiver should begin when the server starts up. If the TECHOST option is specified, TECBEGINEVENTLOGGING defaults to YES.

Syntax

```
>>-TECBegineventlogging--+-Yes-+-------------------------------><
                         '-No--'
```

Parameters

Yes
: Specifies that event logging begins when the server starts up and if a TECHOST option is specified.

No
: Specifies that event logging should not begin when the server starts up. To later begin event logging to the TIVOLI receiver (if the TECHOST option has been specified), you must issue the BEGIN EVENTLOGGING command.

Examples

```
tecbegineventlogging yes
```

TECHOST

The TECHOST option specifies the host name or IP address for the Tivoli® event server.

Syntax

```
>>-TECHost--host_name-----------------------------------------><
```

Parameters

host_name
: Specifies the host name or IP address for the Tivoli event server.

Examples

```
techost 9.114.22.345
```

TECPORT

The TECPORT option specifies the TCP/IP port address on which the Tivoli® event server is listening. This option is only required if the Tivoli event server is on a system that does not have a Port Mapper service running.

Syntax

```
>>-TECPort--port_number---------------------------------------><
```

Parameters

port_number
: Specifies the Tivoli event server port address. The value must be between 0 and 32767. AIX Linux This option is not required.

Examples

```
tecport 1555
```

TECUTF8EVENT

The TECUTF8EVENT option allows the IBM Spectrum Protect™ administrator to send information to the Tivoli Enterprise Console® (TEC) server in UTF–8 data format. The default is No. You can display whether or not this option is enabled by issuing the QUERY OPTION command.

Syntax

```
>>-TECUTF8event--+-Yes-+---------------------------------------><
                '-No--'
```

Parameters

Yes
: Specifies that the IBM Spectrum Protect server will encode the TEC event into UTF–8 before issuing the event to the TEC server.

No
: Specifies that IBM Spectrum Protect server will not encode the TEC event into UTF–8 and it will be issued to the TEC server in ASCII format.

Examples

```
tecutf8event yes
```

THROUGHPUTDATATHRESHOLD

The THROUGHPUTDATATHRESHOLD option specifies a throughput threshold that a client session must reach to prevent being canceled after the time threshold is reached.

This option is used in conjunction with the THROUGHPUTTIMETHRESHOLD server option, which sets the value for the time threshold plus the media wait time. The time threshold starts when the client begins sending data to the server for storage (as opposed to setup or session housekeeping data).

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-THROUGHPUTDatathreshold-- kilobytes_per_second--------------><
```

Parameters

kilobytes_per_second
: Specifies the throughput that client sessions must achieve to prevent cancellation after THROUGHPUTTIMETHRESHOLD minutes have elapsed. This threshold does not include time spent waiting for media mounts. A value of 0 prevents examining client sessions for insufficient throughput. Throughput is computed by adding send and receive byte counts and dividing by the length of the session. The length does not include time spent waiting for media mounts and starts at the time a client sends data to the server for storage. The default is 0. The minimum value is 0; the maximum is 99999999.

Examples

Specify that the server is to wait until 90 minutes plus the media wait time after a session has started sending data before storage examines it as a candidate for cancellation due to low throughput. If a session is not achieving 50 KB per second in transfer rates, it will be canceled.

```
throughputtimethreshold 90
Throughputdatathreshold 50
```

THROUGHPUTTIMETHRESHOLD

The THROUGHPUTTIMETHRESHOLD option specifies the time threshold for a session after which it may be canceled for low throughput.

You can update this server option without stopping and restarting the server by using the SETOPT command. See SETOPT (Set a server option for dynamic update).

Syntax

```
>>-THROUGHPUTTimethreshold--minutes----------------------------><
```

Parameters

minutes
: Specifies the threshold for examining client sessions and canceling them if the data throughput threshold is not met (see the THROUGHPUTDATATHRESHOLD server option). This threshold does not include time spent waiting for media mounts. The time threshold starts when a client begins sending data to the server for storage (as opposed to setup or session housekeeping data). A value of 0 prevents examining client sessions for low throughput. The default is 0. The minimum value is 0; the maximum is 99999999.

Examples

Specify that the server is to wait until 90 minutes plus the media wait time after a session has started sending data before examining it as a candidate for cancellation. If a session is not achieving 50 thousand bytes per second in transfer rates, it will be canceled.

```
throughputtimethreshold 90
Throughputdatathreshold 50
```

Windows

TIMEFORMAT

The TIMEFORMAT option specifies the format in which time is displayed by the server.

The value for the TIMEFORMAT option is overridden by the time formatting definition of the locale if the locale is successfully initialized at server startup. The locale is specified in the LANGUAGE option.

Syntax

```
>>-TIMEformat--format_number-----------------------------------><
```

Parameters

format_number
: Select a number from 1 to 4 to identify the time format used by the server. The default is 1.

  1
  : hh:mm:ss

  2
  : hh,mm,ss

  3
  : hh.mm.ss

  4
  : hh:mm:ss a.m or p.m.

  5
  : a.m or p.m. hh:mm:ss

Examples

```
timeformat 4
```

TXNGROUPMAX

The TXNGROUPMAX option specifies the number of objects that are transferred as a group between a client and the server between transaction commit points. The minimum value is 4 objects and the maximum value is 65000 objects. The default value is 4096 objects. The objects transferred are actual files, directories, or both. The server counts each file or directory as one object.

It is possible to affect the performance of client backup, archive, restore, and retrieve operations by using a larger value for this option:

1. If you increase the value of the TXNGROUPMAX option by a large amount, watch for possible effects on the recovery log. A larger value for the TXNGROUPMAX option can result in increased utilization of the recovery log, as well as an increased length of time for a transaction to commit. If the effects are severe enough, they can lead to problems with operation of the server.
2. Increasing the value of the TXNGROUPMAX option can improve throughput for operations storing data directly to tape, especially when storing a large number of objects. However, a larger value of the TXNGROUPMAX option can also increase the number of objects that must be resent in the case where the transaction is stopped because an input file changed during backup, or because a new storage volume was required. The larger the value of the TXNGROUPMAX option, the more data must be resent.
3. Increasing the TXNGROUPMAX value will affect the responsiveness of stopping the operation and the client may will have to wait longer for the transaction to complete.

You can override the value of this option for individual client nodes. See the TXNGROUPMAX parameter in REGISTER NODE (Register a node) and UPDATE NODE (Update node attributes).

This option is related to the TXNBYTELIMIT option in the client options file. TXNBYTELIMIT controls the number of bytes, as opposed to the number of objects, that are transferred between transaction commit points. At the completion of transferring an object, the client commits the transaction if the number of bytes transferred during the transaction reaches or exceeds the value of TXNBYTELIMIT, regardless of the number of objects transferred.

Syntax

```
>>-TXNGroupmax--number_of_objects------------------------------><
```

Parameters

number_of_objects
: Specifies a number from 4 to 65000 for the maximum number of objects per transaction. The default is 4096.

Examples

```
txngroupmax 4096
```

UNIQUETDPTECEVENTS

The UNIQUETDPTECEVENTS option generates a unique Tivoli Enterprise Console® (TEC) event class for each individual IBM Spectrum Protect™ message, including client, server, and IBM Spectrum Protect Data Protection client messages. The default is No.

Syntax

```
>>-UNIQUETDPtecevents--+-Yes-+---------------------------------><
                       '-No--'
```

Parameters

Yes
: Specifies that unique IBM Spectrum Protect Data Protection messages are sent to the TEC event server. Dynamically sets UNIQUETECevents to YES.

No
: Specifies that general messages are sent to the TEC event server.

Examples

```
uniquetdptecevents yes
```

UNIQUETECEVENTS

The UNIQUETECEVENTS option generates a unique Tivoli Enterprise Console® (TEC) event class for each individual IBM Spectrum Protect™ message. The default is No.

Syntax

```
>>-UNIQUETECevents--+-Yes-+-----------------------------------><
                    '-No--'
```

Parameters

Yes
: Specifies that unique messages are sent to the TEC event server.

No
: Specifies that general messages are sent to the TEC event server.

Examples

```
uniquetecevents yes
```

USEREXIT

The USEREXIT option specifies a user-defined exit that will be given control to manage an event.

Syntax

```
                                    (1)            (2)
>>-USEREXIT--+-Yes-+--module_name------DLL_name-----------------><
             '-No--'

             (3)
>--function-------------------------------------------------------><
```

Notes:

1. *module_name* is available only on AIX, HP-UX, Linux, Solaris, and z/OS.
2. *DLL_name* is available only on Windows.
3. *function* is available only on Windows.

Parameters

Yes
: Specifies that event logging to the user exit receiver begins automatically at server startup.

No
: Specifies that event logging to the user exit receiver does not begin automatically at server startup. When this parameter has been specified, you must begin event logging manually by issuing the BEGIN EVENTLOGGING command.

AIX Linux module_name
: AIX Linux Specifies the module name of the user exit.

  AIX Linux This is the name of a shared library containing the exit. The module name can be either a fully qualified path name or just the module name itself. If it is just the module name, it is loaded from the current directory.

Windows DLL_name
: Windows Specifies the DLL name that contains the user-exit function.

Windows function

Windows Specifies the name of the user-exit function in the DLL.

Examples

Windows

```
userexit yes dllname.dll dllmodulename
```

AIX Linux

```
userexit yes fevent.exit
```

VERBCHECK

The VERBCHECK option specifies that the server will do additional error checking on the structure of commands sent by the client. This option should only be enabled when the client sends incorrectly formed requests to the server, causing the server to crash. When this option is enabled, you will get a protocol error instead of a server crash.

Syntax

```
>>-VERBCHECK-------------------------------------------------><
```

Parameters

None

Examples

Enable additional error checking for commands sent by the client:

```
verbcheck
```

VOLUMEHISTORY

The VOLUMEHISTORY option specifies the name of files to be automatically updated whenever server sequential volume history information is changed. There is no default for this option.

You can include one or more VOLUMEHISTORY options in the server options file. When you use multiple VOLUMEHISTORY options, the server automatically updates and stores a backup copy of the volume history information in each file you specify.

Syntax

```
>>-VOLUMEHistory--file_name-----------------------------------><
```

Parameters

file_name
: Specifies the name of the file where you want the server to store a backup copy of the volume history information that it collects.

Examples

```
volumehistory volhist.out
```

Server utilities

Use server utilities to perform special tasks on the server while the server is not running.

- Windows DSMMAXSG (Increase the block size for writing data)
  Use the DSMMAXSG utility to increase the maximum transfer length for host bus adapters (HBAs). As a result, the block size that is used by the IBM Spectrum Protect™ server for writing data to and getting data from certain types of tape drives is increased.
- DSMSERV (Start the server)
  Use this utility to start the IBM Spectrum Protect server.
- AIX Linux Server startup script: rc.dsmserv
  You can use the rc.dsmserv script in your system startup to automatically start a server instance under a specific user ID.
- Linux Server startup script: dsmserv.rc
  You can use the dsmserv.rc script to stop a server instance, or to manually or automatically start a server.
- DSMSERV DISPLAY DBSPACE (Display information about database storage space)
  Use this utility to display information about storage space that is defined for the database. The output of this utility is the same as the output of the QUERY DBSPACE command, but you can use this utility when the server is not running.
- DSMSERV DISPLAY LOG (Display recovery log information)
  Use this utility to display information about recovery logs including the active log, the mirror for the active log, the failover directory for the archive log, and the overflow location for logs. Use this utility when the server is not running.
- DSMSERV EXTEND DBSPACE (Increase space for the database)
  Use this utility to increase space for the database by adding directories for the database to use. This utility performs the same function as the EXTEND DBSPACE command, but you can use it when the server is not running.
- DSMSERV FORMAT (Format the database and log)
  Use the DSMSERV FORMAT utility to initialize the server database and recovery log. No other server activity is allowed while initializing the database and recovery log.
- DSMSERV INSERTDB (Move a server database into an empty database)
  Use the DSMSERV INSERTDB utility to move a server database into a new database. The database can be extracted from the original server and inserted into a new database on the new server by using a network connection between the two servers. The database can also be inserted from media that contains the extracted database.
- DSMSERV LOADFORMAT (Format a database)
  Use the DSMSERV LOADFORMAT utility when upgrading from Version 5. The utility formats an empty database in preparation for inserting an extracted database into the empty database.
- DSMSERV REMOVEDB (Remove a database)
  Use the DSMSERV REMOVEDB utility to remove an IBM Spectrum Protect server database.
- DSMSERV RESTORE DB (Restore the database)
  Use this utility to restore a database by using a database backup.
- Windows DSMSERV UPDATE (Create registry entries for a server instance)
  Use this utility to create registry entries for an IBM Spectrum Protect server instance if the entries were accidentally deleted.
- AIX Linux DSMULOG (Capture IBM Spectrum Protect server messages to a user log file)
  Use this command to capture IBM Spectrum Protect server console messages to a user log file. You can specify that IBM Spectrum Protect writes messages to more than one user log file.

Windows

DSMMAXSG (Increase the block size for writing data)

Use the DSMMAXSG utility to increase the maximum transfer length for host bus adapters (HBAs). As a result, the block size that is used by the IBM Spectrum Protect™ server for writing data to and getting data from certain types of tape drives is increased.

With this utility, the maximum block size that you can specify is 256 KB. Depending on your system environment, increasing the block size can improve the rate at which IBM Spectrum Protect processes data for backup and restore operations and for archive and retrieve operations. However, the utility does not affect the generation of backup sets.

You can use tape drives that are only attached to SCSI or Fibre Channel HBAs and that have the following device types:

- 3590
- 3592
- DLT
- ECARTRIDGE
- LTO

The utility runs automatically as part of the IBM Spectrum Protect server and storage agent installation. However, if you install a new HBA on your system after you install a server or storage agent, or if you install a new version of an existing HBA device driver that resets the value of the maximum transfer size, you must run the utility manually to take advantage of the larger block size.

When you run this utility, it modifies one registry key for every HBA driver on the system. The name of the key is MaximumSGList.

Restriction: If data is backed up or archived to tape using the 256 KB block size, the tape cannot be appended to or read from using an HBA that does not support the 256 KB block size. For example, if you use a 256 KB Windows system to back up client data to the IBM Spectrum Protect server, you cannot restore the data using a Windows system that supports a different transfer length. To append to or read from tape written to using a 256 KB transfer length, you must install an HBA that supports 256 KB transfers.

Syntax

```
>>-dsmmaxsg---------------------------------------------------><
```

Example: Increase the block size for writing data

Run the DSMMAXSG utility to increase the block size that is used by the IBM Spectrum Protect.

```
dsmmaxsg
```

DSMSERV (Start the server)

Use this utility to start the IBM Spectrum Protect™ server.

Restrictions:

- Do not enter more than 1022 characters in the DSMSERV console command-line interface. Text that exceeds 1022 characters is truncated.
- Windows The following parameters are mutually exclusive:
  - NOEXPIRE
  - RUNFILE
  - MAINTENANCE

AIX | Linux | Windows

Syntax

Notes:

1. This parameter applies only to AIX® and Linux servers.
2. This parameter applies only to Windows servers.
3. This parameter applies only to Windows servers.
4. This parameter applies only to AIX, Linux, and Windows servers.

AIX Linux Windows

Parameters

AIX Linux -u user_name

AIX Linux Specifies a user name to switch to before you start the server. To start the server from the root user ID, you must specify the -u parameter and follow the instructions in Starting the server from the root user ID.

AIX Linux -i instance_dir

AIX Linux Specifies an instance directory to use. The instance directory becomes the current working directory of the server.

Windows -k key_name

Windows Specifies the name of the Windows registry key from which to retrieve information about the server. The default is Server1.

AIX Linux -noexpire

AIX Linux Specifies that the server does not remove expired files from the server database. The files are not deleted from server storage when you start the server.

Windows NOEXPIRE

Windows Specifies that the server does not remove expired files from the server database. The files are not deleted from server storage when you start the server.

-o options_file

Specifies an options file to use.

AIX Linux -quiet

AIX Linux Specifies that messages to the console are suppressed.

AIX Linux Windows MAINTenance

AIX Linux Windows Specifies that the server is started in maintenance mode, and that administrative command schedules, client schedules, client sessions, storage-space reclamation, inventory expiration, and storage-pool migration are disabled.

Tip: Maintenance mode is the preferred method for running the server during maintenance or reconfiguration tasks. When you run the server in maintenance mode, operations that might disrupt maintenance or reconfiguration tasks are disabled automatically.

RUNFILE file_name

Specifies the name of a text file to be run on the server. The file contains a list of server commands.

Attention: Whenever the RUNFILE parameter is used, the server halts when processing is complete. You must restart the server by using the DSMSERV utility.

Example: Start the server

Start the server for normal operation. Issue the following command on one line:

AIX

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
usr/bin/dsmserv
```

AIX Ensure that you include a space after `SHMPSIZE=64K`. By starting the server with this command, you enable 64 KB memory pages for the server. This setting helps you optimize server performance.

Linux

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Windows

```
C:\Program Files\Tivoli\TSM\bin\dsmserv -k server2
```

Windows

Example: Start an additional server

Start an additional server by using the registry key named SERVER2.

```
dsmserv -k server2
```

AIX Linux Windows

Example: Load the sample script

Load the sample script file that is provided with the server.

```
dsmserv runfile scripts.smp
```

AIX | Linux | Windows

Example: Start the server in maintenance mode

Before you begin maintenance or reconfiguration tasks, start the server in maintenance mode.

```
dsmserv maintenance
```

Related tasks:
Starting the server in maintenance mode
AIX

Server startup script: rc.dsmserv

You can use the rc.dsmserv script in your system startup to automatically start a server instance under a specific user ID.

Syntax

```
>>-rc.dsmserv--+- -u--user_name-+--+-------------------+-------><
               '- -U--user_name-'  '- -i--instance_dir-'
```

Parameters

-u user_name
: Specifies the instance user ID for which the environment is set up. The server will run under this user ID.

-U user_name
: Specifies the instance user ID for which the environment is set up. The server will run under the user ID of the invoker of the command.

-i instance_dir
: Specifies an instance directory, which becomes the working directory of the server.

Related tasks:
AIX: Automatically starting servers
Linux

Server startup script: dsmserv.rc

You can use the dsmserv.rc script to stop a server instance, or to manually or automatically start a server.

Prerequisites

Before you issue the DSMSERV.RC command, complete the following steps:

1. Ensure that the server instance runs under a non-root user ID with the same name as the instance owner.
2. Copy the dsmserv.rc script to the /etc/rc.d/init.d directory. The dsmserv.rc script is in the server installation directory, for example, /opt/tivoli/tsm/server/bin.
3. Rename the script so that it matches the name of the server instance owner, for example, `tsminst1`.
4. If the server instance directory is not home_directory/tsminst1, locate the following line in the script copy:

   ```
   instance_dir="${instance_home}/tsminst1"
   ```

   Change the line so that it points to your server instance directory, for example:

   ```
   instance_dir="/tsminst1"
   ```

5. In the script copy, locate the following line:

   ```
   # pidfile: /var/run/dsmserv_instancename.pid
   ```

Change the instance name value to the name of the server instance owner. For example, if the server instance owner is tsminst1, update the line as shown:

```
# pidfile: /var/run/dsmserv_tsminst1.pid
```

6. Use tools such as the CHKCONFIG utility to configure the run level in which the server automatically starts. Specify a value that corresponds to a multiuser mode, with networking turned on. Typically, the run level to use is 3 or 5, depending on the operating system and its configuration. For details about run levels, see the documentation for your operating system.

Syntax

```
>>-dsmserv.rc--+---------+-------------------------------------><
               +-start---+
               +-stop----+
               +-status--+
               '-restart-'
```

Parameters

start
: Starts the server.

stop
: Stops the server.

status
: Shows the status of the server. If the status is `started`, the process ID of the server process is also shown.

restart
: Stops the server and starts it again.

Related tasks:

Linux: Automatically starting servers on Linux systems

DSMSERV DISPLAY DBSPACE (Display information about database storage space)

Use this utility to display information about storage space that is defined for the database. The output of this utility is the same as the output of the QUERY DBSPACE command, but you can use this utility when the server is not running.

Syntax

```
>>-DSMSERV -+----------------------+----------------------------->
            |  (1)                 |
            '------- -u--user_name-'

                                (2).- -k--Server1--.
>--+-------------------------+------+---------------+----------->
   |  (1)                    |      '- -k--key_name-'
   '------- -i--instance_dir-'

>--+-------------------+--+------------+--+---------+----------->
   '- -o--options_file-'  '- -noexpire-'  '- -quiet-'

>--DISPlay DBSPace-----------------------------------------------><
```

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX | Linux -u user_name

AIX Linux Specifies a user name to switch to before initializing the server.

AIX Linux -i instance_dir

AIX Linux Specifies an instance directory to use. This becomes the current working directory of the server.

Windows -k key_name

Windows Specifies the name of a Windows registry key that is used to store information about this server. Use this parameter only when there is more than one server on the same system. The default value is SERVER1.

-o options_file

Specifies an options file to use.

-noexpire

Specifies that expiration processing is suppressed when starting.

-quiet

Specifies that messages to the console are suppressed.

Example: Display database space information

Display information about database storage space. See Field descriptions for details about the information shown in the output. Issue the command.

```
dsmserv display dbspace
```

AIX Linux

```
Location        Total Space (MB)   Used Space (MB)   Free Space (MB)
-------------   ----------------   ---------------   ---------------
 /tsmdb001             46,080.00         20,993.12         25,086.88
 /tsmdb002             46,080.00         20,992.15         25,087.85
```

Windows

```
Location          Total Space (MB)   Used Space (MB)   Free Space (MB)
-------------   ----------------   ---------------   ---------------
d:\tsm\db001           46,080.00         20,993.12         25,086.88
d:\tsm\db002           46,080.00         20,993.15         25,087.85
```

Field descriptions

Location

The directory or path that is used for storing the database

Total Space (MB)

The total number of megabytes in the location

Used Space (MB)

The number of megabytes in use in the location

Free Space (MB)

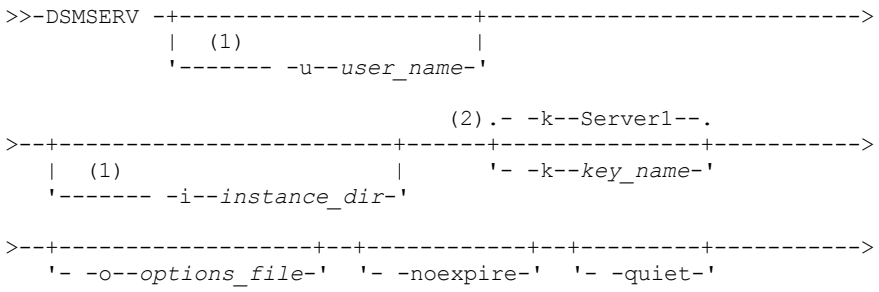
AIX Linux The space remaining in the file system where the path is located

Windows The space remaining on the drive where the directory is located

DSMSERV DISPLAY LOG (Display recovery log information)

Use this utility to display information about recovery logs including the active log, the mirror for the active log, the failover directory for the archive log, and the overflow location for logs. Use this utility when the server is not running.

Syntax



```
>--DISPLAY LOG-----------------------------------------------><
```

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name
AIX Linux Specifies a user name to switch to before initializing the server.
AIX Linux -i instance_dir
AIX Linux Specifies an instance directory to use. This becomes the current working directory of the server.
Windows -k key_name
Windows Specifies the name of the Windows registry key from which to retrieve information about the server. Use this parameter only when there is more than one server on the same system. The default is SERVER1.
-o options_file
Specifies an options file to use.
-noexpire
Specifies that expiration processing is suppressed when starting.
-quiet
Specifies that messages to the console are suppressed.

Examples: Display recovery log information

Display information about the recovery logs. See Field descriptions for details about the information shown in the output.

```
dsmserv display log
```

AIX Linux

```
               Total Space(MB): 38,912
                Used Space(MB): 401.34
                Free Space(MB): 38,358.65
          Active Log Directory: /activelog
         Archive Log Directory: /archivelog
          Mirror Log Directory: /mirrorlog
Archive Failover Log Directory: /archfailoverlog
```

Windows

```
               Total Space(MB): 38,912
                Used Space(MB): 401.34
                Free Space(MB): 38,358.65
          Active Log Directory: h:\tsm\activelog
         Archive Log Directory: k:\tsm\archivelog
          Mirror Log Directory: i:\tsm\mirrorlog
Archive Failover Log Directory: j:\tsm\archfailoverlog
```

Field descriptions

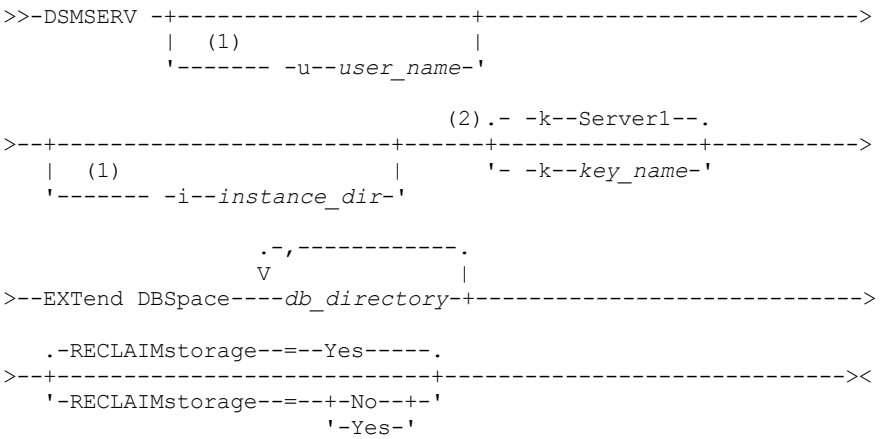
Total Space
Specifies the maximum size of the active log.
Used Space
Specifies the total amount of active log space currently used in the database, in megabytes.
Free Space
Specifies the amount of active log space in the database that is not being used by uncommitted transactions, in megabytes.
Active Log Directory
Specifies the location where active log files are stored. When you change the active log directory, the server moves all archived logs to the archive log directory and all active logs to a new active log directory.
Mirror Log Directory
Specifies the location where the mirror for the active log is maintained.
Archive Failover Log Directory
Specifies the location in which the server saves archive logs if the logs cannot be archived to the archive log destination.

DSMSERV EXTEND DBSPACE (Increase space for the database)

Use this utility to increase space for the database by adding directories for the database to use. This utility performs the same function as the EXTEND DBSPACE command, but you can use it when the server is not running.

Restriction: Redistribution of data and reclaiming of space as part of an operation to extend database space only works with DB2® Version 9.7 or later table spaces, which are created when you format a new Version 6.3 or later server.

Syntax



Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name

AIX Linux Specifies a user name to switch to before you initialize the server.

AIX Linux -i instance_dir

AIX Linux Specifies an instance directory to use. This becomes the current working directory of the server.

Windows -k key_name

Windows Specifies the name of a Windows registry key that is used to store information about this server. Use this parameter only when there is more than one server on the same system. The default value is SERVER1.

db_directory (Required)

Specifies the directories for database storage. The directories must be empty and accessible by the user ID of the database manager. A directory name must be a fully qualified name and cannot exceed 175 characters in length. Enclose the name in quotation marks if it contains embedded blanks, an equal sign, or other special characters. If you are specifying a list of directories for database storage, the maximum length of the list can be 1400 characters.

Windows Restriction: You cannot specify Universal Naming Convention (UNC) paths.

Tip: Specify directories that are the same size as existing directories to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

RECLAIMstorage

Specifies whether data is redistributed across newly created database directories and space is reclaimed from the old storage paths when you add space to the database. This parameter is optional. The default value is Yes.

Yes

Specifies that data is redistributed so that new directories are available for immediate use.

Important: The redistribution process uses considerable system resources so ensure that you plan ahead. Also, the server might be offline for a while, until the process is completed.

No

Specifies that data is not redistributed across database directories and storage space is not reclaimed.

AIX Linux

Example: Increase space for the database

Add a directory named stg1 in the tsm_db directory for the database storage space and then redistribute data and reclaim space by issuing the following command:

```
dsmserv extend dbspace /tsm_db/stg1
```

Windows

Example: Increase space for the database

Add drive D to the storage space for the database and then redistribute data and reclaim space by issuing the following command:

```
dsmserv extend dbspace D:
```

Related reference:
EXTEND DBSPACE (Increase space for the database)

DSMSERV FORMAT (Format the database and log)

Use the DSMSERV FORMAT utility to initialize the server database and recovery log. No other server activity is allowed while initializing the database and recovery log.

The directories that are specified in this utility should be on fast, reliable storage. Do not place the directories on file systems that might run out of space. If certain directories (for example, the active log directory) become unavailable or full, the server stops.

Windows Restriction: If you are using a File Allocation Table (FAT or FAT32) or a New Technology File System (NTFS) format, you cannot specify the root directory of that system as the location of a database directory or log directory. Instead, you must create one or more subdirectories within the root directory. Then, create the database directories and log directories within the subdirectories.

Windows Important: The installation program creates a set of registry keys. One of these keys points to the directory where a default server, named SERVER1, is created. To install an extra server, create a directory and use the DSMSERV FORMAT utility, with the -k parameter, from that directory. That directory becomes the location of the server. The registry tracks the installed servers.

When a server is initially created by using the DSMSERV FORMAT utility or the configuration wizard, a server database and recovery log are created. In addition, files are created to hold database information that is used by the database manager.

Syntax

```
>--+-----------------------------------+------------------------><
   '-MIRRorlogdirectory--=--directory-'
```

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name

AIX Linux Specifies a user name to switch to before initializing the server. This parameter is optional.

AIX Linux -i instance_dir

AIX Linux Specifies an instance directory to use. This directory becomes the current working directory of the server. This parameter is optional.

Windows -k key_name

Windows Specifies the name of a Windows registry key that is used to store information about this server. Use this parameter only to install extra servers on the same system. After you install a server by using this parameter, you must always start it with the value of this parameter. This parameter is optional. The default is SERVER1.

Restriction: Additional instances of the IBM Spectrum Protect™ server that are running on the same system will compete for resources and impact overall performance of each IBM Spectrum Protect server.

-o options_file

Specifies an options file to use. This parameter is optional.

-noexpire

Specifies that expiration processing is suppressed when starting. This parameter is optional.

-quiet

Specifies that messages to the console are suppressed. This parameter is optional.

DBDir

Specifies the relative path names of one or more directories that are used to store database objects. Directory names must be separated by commas but without spaces. You can specify up to 128 directory names. You must specify either the DBDIR or the DBFILE parameter.

Tip: If you specify multiple directories, ensure that the underlying file systems are of equal size to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

DBFile

Specifies the name of a file that contains the relative path names of one or more directories that are used to store database objects. Each directory name must be on a separate line in the file. You can specify up to 128 directory names. You must specify either the DBDIR or the DBFILE parameter.

ACTIVELOGSize

Specifies the size of the active log file in megabytes. This parameter is optional. The minimum value is 2048 MB (2 GB); the maximum is 524,288 MB (512 GB). If an odd number is specified, the value is rounded up to the next even number. The default is 16384 MB.

The size of an active log file is based on the value of the ACTIVELOGSIZE option. Guidelines for space requirements are in the following table:

Table 1. How to estimate volume and file space requirements

ACTIVELOGSize option value	**Reserve this much free space in the active log directory, in addition to the ACTIVELOGSize space**
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Required)

Specifies the directory in which the server writes and stores active log files. There is only one active log location. The name must be a fully qualified directory name. The directory must exist, it must be empty, and it must be accessible by the user ID of the database manager. The maximum number of characters is 175.

ARCHLogdirectory (Required)

Specifies the directory for the archive log files. The name must be a fully qualified directory name. The maximum number of characters is 175.

ARCHFailoverlogdirectory

Specifies the directory to be used as an alternative storage location if the ARCHLOGDIRECTORY directory is full. This parameter is optional. The maximum number of characters is 175.

MIRRorlogdirectory

Specifies the directory in which the server mirrors the active log (those files in the ACTIVELOGDIRECTORY directory). This parameter is optional. The directory must be a fully qualified directory name. The maximum number of characters is 175.

Example: Format a database

AIX | Linux

```
dsmserv format dbdir=/tsmdb001 activelogsize=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Windows

```
dsmserv -k server2 format dbdir=d:\tsm\db001 activelogsize=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

DSMSERV INSERTDB (Move a server database into an empty database)

Use the DSMSERV INSERTDB utility to move a server database into a new database. The database can be extracted from the original server and inserted into a new database on the new server by using a network connection between the two servers. The database can also be inserted from media that contains the extracted database.

Before you use the DSMSERV INSERTDB utility, complete the planning and preparation tasks, such as backing up the database and saving configuration information. Ensure that you meet all requirements before you move the server database.

Requirements for insertion by using media

Before you run the utility to insert the server database into an empty database, ensure that your system meets the following requirements.

- The manifest file from the DSMUPGRD EXTRACTDB operation must be available.
- If the manifest file does not contain device configuration information, or if you are specifying the CONFIGINFO=DEVCONFIG parameter, both of the following statements must be true:
  - The server options file must contain an entry for the device configuration file.
  - The device configuration file must have information about the device class that is specified in the manifest file.
- The media that contains the extracted database must be available to the V8 server. Also, the permissions must be set to grant access to the media for the user ID that owns the V8 server instance.

Syntax

```
>>-DSMSERV -+----------------------+---------------------------->
            |  (1)                 |
            '------- -u--user_name-'

                                (2).- -k--Server1--.
>--+-------------------------+------+---------------+----------->
   |  (1)                    |      '- -k--key_name-'
   '------- -i--instance_dir-'

>--+-------------------+--+------------+--+---------+----------->
   '- -o--options_file-'  '- -noexpire-'  '- -quiet-'

>--INSERTDB--+-| A: Insert from media |-----+------------------->
             '-| B: Insert over a network |-'

   .-PREview--=--No------.
>--+--------------------+-------------------------------------><
   '-PREview--=--+-Yes-+-'
                 '-No--'

A: Insert from media

|--+-------------------------------+-------------------------->
```

```
   '-DEVclass--=--device_class_name-'

   .-CONFiginfo--=--MANifest------.
>--+-----------------------------+--MANifest--=--file_name-----|
   '-CONFiginfo--=--+-MANifest--+-'
                    '-DEVconfig-'

B: Insert over a network

   .-SESSWait--=--60------.
|--+----------------------+-----------------------------------|
   '-SESSWait--=--minutes-'
```

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name
AIX Linux Specifies a user name to switch to before initializing the server. This parameter is optional.

AIX Linux -i instance_dir
AIX Linux Specifies an instance directory to use. This directory becomes the current working directory of the server. This parameter is optional.

Windows -k key_name
Windows Specifies the name of the Windows registry key from which to retrieve information about the server. This parameter is optional. The default is SERVER1.

-o options_file
Specifies an options file to use. This parameter is optional.

-noexpire
Specifies that expiration processing is suppressed when starting. This parameter is optional.

-quiet
Specifies that messages to the console are suppressed. This parameter is optional.

DEVclass
Specifies a sequential-access device class. You can specify any device class except for the DISK device class. The definition for the device class must exist in either the manifest file or the device configuration file.
This parameter is optional and is used only when the database that you want to insert into the empty V8 database was extracted to media. If the database is on media and you do not specify a device class, the device class that is identified in the manifest file is used.
Restriction: You cannot use a device class with a device type of NAS or CENTERA.

MANifest
Specifies the location of the manifest file. Use a fully qualified file name, or place in a local directory. For example:
```
./manifest.txt
```

This parameter is required when the database that you want to insert into the empty V8 database was extracted to media.

CONFiginfo
Specifies the source of the device configuration information that is used by the DSMSERV INSERTDB operation. The default value for this parameter is MANIFEST. Possible values are as follows:

MANifest
Specifies that device configuration information is read from the manifest file. If the manifest file does not have device configuration information, the device configuration file is used instead.

DEVConfig
Specifies that device configuration information is read from the device configuration file.

SESSWait
Specifies the number of minutes that the V8 server waits to be contacted by the original server. The default value is 60 minutes.

Use this parameter only if the data that is inserted into the empty V8 database is transmitted from the source server with a network connection.

PREview

Specifies whether to preview the insertion operation. This parameter is optional. The default value is NO.

Use the PREVIEW=YES parameter to test a database. When you use this parameter, the operation includes all steps of the process, except for the actual insertion of data into the new database. When you preview the insertion operation, you can quickly verify that the source database is readable. You can also identify any data constraint violations that might prevent an upgraded database from being put into production.

DSMSERV LOADFORMAT (Format a database)

Use the DSMSERV LOADFORMAT utility when upgrading from Version 5. The utility formats an empty database in preparation for inserting an extracted database into the empty database.

Syntax

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name
AIX Linux Specifies a user name to switch to before initializing the server. This parameter is optional.

AIX Linux -i instance_dir
AIX Linux Specifies an instance directory to use. This directory becomes the current working directory of the server. This parameter is optional.

Windows -k key_name
Windows Specifies the name of a Windows registry key that is used to store information about this server. Use this parameter only to install additional servers on the same system. After you install a server by using this parameter, you must always start it with the value of this parameter. The default is SERVER1.

-o options_file
Specifies an options file to use. This parameter is optional.

-noexpire
Specifies that expiration processing is suppressed when the server starts. This parameter is optional.

-quiet
Specifies that messages to the console are suppressed. This parameter is optional.

DBDir
Specifies the relative path names of one or more directories that are used to store database objects. Directory names must be separated by commas but without spaces. You can specify up to 128 directory names. You must specify either the DBDIR or the DBFILE parameter.
Tip: If you specify multiple directories, ensure that the underlying file systems are of equal size to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

DBFile
Specifies the name of a file that contains the relative path names of one or more directories that are used to store database objects. Each directory name must be on a separate line in the file. You can specify up to 128 directory names. You must specify either the DBDIR or the DBFILE parameter.

ACTIVELOGSize
Specifies the size of the active log file in megabytes. This parameter is optional. The minimum value is 2048 MB (2 GB); the maximum is 524,288 MB (512 GB). If an odd number is specified, the value is rounded up to the next even number. The default is 16384 MB.
The size of an active log file is based on the value of the ACTIVELOGSIZE option. Guidelines for space requirements are in the following table:

Table 1. How to estimate volume and file space requirements

ACTIVELOGSize option value	Reserve this much free space in the active log directory, in addition to the ACTIVELOGSize space
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Required)
Specifies the directory in which the server writes and stores active log files. There is only one active log location. The name must be a fully qualified directory name. The directory must exist, it must be empty, and it must be accessible by the user ID of the database manager. The maximum number of characters is 175.

ARCHLogdirectory (Required)
Specifies the directory for the archive log files. The name must be a fully qualified directory name. The maximum number of characters is 175.

ARCHFailoverlogdirectory
Specifies the directory to be used as an alternative storage location if the ARCHLOGDIRECTORY directory is full. This parameter is optional. The maximum number of characters is 175.

MIRRorlogdirectory
Specifies the directory in which the server mirrors the active log (those files in the ACTIVELOGDIRECTORY directory). This parameter is optional. The directory must be a fully qualified directory name. The maximum number of characters is 175.

Example: Format a database

AIX | Linux

```
dsmserv loadformat dbdir=/tsmdb001 activelogsize=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Windows

```
dsmserv -k server2 loadformat dbdir=d:\tsm\db001 activelogsize=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

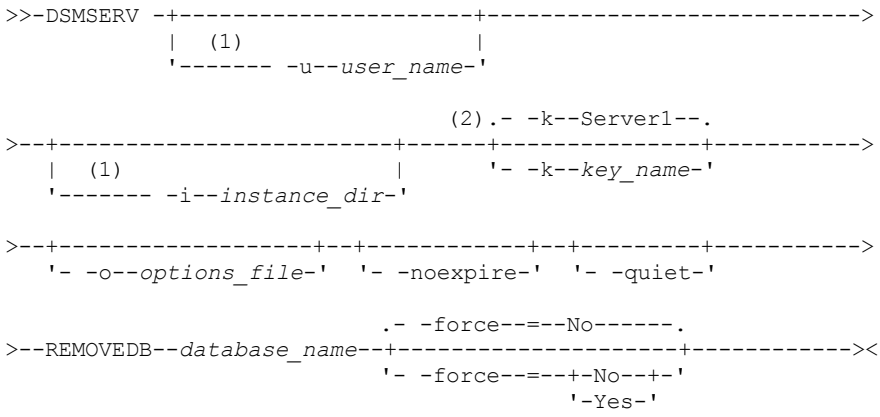
DSMSERV REMOVEDB (Remove a database)

Use the DSMSERV REMOVEDB utility to remove an IBM Spectrum Protect™ server database.

When you run this utility, you delete the server database, active log files, and active log mirror files. However, the archive log files and archive log failover log files are deleted only after you start a point-in-time database restore.

You must halt the IBM Spectrum Protect server before you issue this command.

Syntax



Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name
AIX Linux Specifies a user name to switch to before initializing the server.
AIX Linux -i instance_dir
AIX Linux Specifies an instance directory to use. This becomes the current working directory of the server.
Windows -k key_name
Windows Specifies the name of the Windows registry key from which to retrieve information about the server. The default is SERVER1.
-o options_file
Specifies an options file to use.
-noexpire
Specifies that expiration processing is suppressed when starting.
-quiet
Specifies that messages to the console are suppressed.
database_name
The database name that was entered during installation. If the database was formatted manually, then this is the database name parameter in the DSMSERV FORMAT or DSMSERV LOADFORMAT utility. This database name can also be found in dsmserv.opt file. This parameter is required.
-force
Specifies whether the database is removed when there are open connections. The default is No. This parameter is optional. The values are as follows:

Yes
Specifies that the database is removed regardless of open connections
No
Specifies that the database is removed only when all connections are closed.

Example: Remove a database

Remove the IBM Spectrum Protect server database TSMDB1 and all of its references.

```
dsmserv removedb TSMDB1
```

Example: Remove a database with force parameter

Remove the IBM Spectrum Protect server database TSMDB1 and all of its references, even if it has open connections:

```
dsmserv removedb TSMDB1 force=yes
```

DSMSERV RESTORE DB (Restore the database)

Use this utility to restore a database by using a database backup.

Restriction: You cannot restore a server database if the release level of the server database backup is different from the release level of the server that is being restored. For example, an error occurs when you restore a Version 7.1.3 database and you are using a Version 8.1 IBM Spectrum Protect™ server.

The restore operation uses database backups created with the BACKUP DB command.

Important: After a point-in-time restore operation, issue the AUDIT VOLUME command to audit all DISK volumes and resolve any inconsistencies between database information and storage pool volumes. Before restoring the database, examine the volume history file to find out about any sequential access storage pool volumes that were deleted or reused since the point in time to which the database was restored.

- DSMSERV RESTORE DB (Restore a database to its most current state)
  Use the DSMSERV RESTORE DB utility to restore a database to its most current state under certain conditions.
- DSMSERV RESTORE DB (Restore a database to a point-in-time)
  Use this command to restore a database to a point in time. A volume history file and a device configuration file must be available.

DSMSERV RESTORE DB (Restore a database to its most current state)

Use the DSMSERV RESTORE DB utility to restore a database to its most current state under certain conditions.

The following conditions must be met:

- An intact volume history file is available.
- The recovery logs are available.
- A device configuration file with the applicable device information is available.

Restriction: You cannot restore a server database if the release level of the server database backup is different from the release level of the server that is being restored. For example, an error occurs when you restore a Version 7.1.3 database and you are using a Version 8.1 IBM Spectrum Protect™ server.

IBM Spectrum Protect requests volume mounts to load the most recent backup series and then uses the recovery logs to update the database to its most current state.

Snapshot database backups cannot be used to restore a database to its most current state.

Syntax

```
   .-RESTOREKeys--=--No-------.
>--+--------------------------+--------------------------------->
   '-RESTOREKeys--=--+-No---+-'
                     +-YES--+
                     '-ONLY-'

>--+-----------------------------+------------------------------><
   '-PASSword--=--password_name-'
```

Notes:

1. This parameter applies to AIX® and Linux servers only.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name
AIX Linux Specifies a user name to switch to before initializing the server.

AIX Linux -i instance_dir
AIX Linux Specifies an instance directory to use. This instance directory becomes the current working directory of the server.

Windows -k key_name
Windows Specifies the name of the Windows registry key from which to retrieve information about the server. The default is SERVER1.

-o options_file
Specifies an options file to use.

AIX Linux -quiet
AIX Linux Specifies that messages to the console are suppressed.

RECOVerydir
Specifies a directory in which to store recovery log information from the database backup media. This directory must have enough space to hold this transaction recovery information and must be an empty directory. If this parameter is not specified, the default is to the directory specified by one of the following parameters in the DSMSERV FORMAT or DSMSERV LOADFORMAT utility:

- ARCHFAILOVERLOGDIRECTORY, if specified
- ARCHLOGDIRECTORY, if ARCHFAILOVERLOGDIRECTORY is not specified

ACTIVELOGDir
Specifies a directory in which to store the log files that are used to track the active database operations. This directory must be specified only if the intent is to switch to an active log directory different from the one that had already been configured.

On
Specifies a file that lists the directories to which the database is restored. Specify each directory on a separate line in the file. For example, the ON parameter specifies the restorelist.txt file, which contains the following list: AIX Linux

```
/tsmdb001
/tsmdb002
/tsmdb003
```

Windows

```
e:\tsm\db001
f:\tsm\db002
g:\tsm\db003
```

If this parameter is not specified, the original directories that were recorded in the database backup are used.
Tip: If you specify multiple directories, ensure that the underlying file systems are of equal size to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

PReview
Specifies that the volume history files be examined and that the database backup volumes from the volume history file be evaluated.

1. Which set of database backup volumes best meets the most current criteria that are specified for restore processing? The volume history information provides details about the backup series ID, the operation ID (full, incremental 1, incremental 2, and so on), the date of the database backup, and the device class. This information and the parameters that are specified in the DSMSERV RESTORE DB command determine what to use to perform the

restore. The volume history file is examined to find the most recent database backup and then to restore the data by using that backup.

2. Is self-describing data available for the selected set of database backup volumes? Cross-check the volume history information for this backup series. The reconciliation reports what the self-describing data contains compared to what was learned from the volume history entries. The cross-check involves mounting one or more of the volumes that are indicated by the volume history. Then, using the self-describing data that was included in the database backup volumes, that information is reconciled against what is in the volume history for the database backup. If the information from the volume history file is inconsistent with the self-describing data, then messages are issued to identify the problem. For example, not all values are specified and available, and no self-describing data is found.

If the volume history information is consistent with self-describing data from the database backup, a message is issued indicating that the database backup can be used for restore processing.

If the volume history information is inconsistent with the self-describing data from the database backup or if the self-describing data for the backup cannot be found, error messages are issued indicating what was checked and what was missing.

If the PREVIEW parameter is not specified or if it is set to NO, and if the volume history and self-describing data from the database backup are consistent, then the restore proceeds.

If the PREVIEW parameter is not specified or if it is set to NO, and the reconciliation and validation fail, the database restore is not performed. Make extra volumes available and referred to from the volume history file, or remove the incomplete backup series or operation so that the IBM Spectrum Protect server selects a different preferred series or operation and continues processing.

If the PREVIEW parameter is set to YES, the process performs only the evaluation of the volume history file and the reconciliation and validation against the selected database backup.

AIX Linux Windows RESTOREKeys

AIX Linux Windows Specifies whether to restore the server master encryption key that is used to encrypt storage pool data when the database is restored. This parameter is optional and only applies if you are using encrypted container storage pools in a cloud environment. If the server master key is protected when the database is restored, the default is YES. If the server master key is not protected when the database is restored, the default is NO. You can specify one of the following values:

No
: Specifies that the server master key is not restored when the database is restored.

Yes
: Specifies that the server master key is restored when the database is restored. You must specify a password with this parameter.

Only
: Specifies that only the server master key is restored. The database is not restored.

AIX Linux Windows PASSword

AIX Linux Windows Specifies the password that is used to protect the database backup. This parameter only applies if you are using encrypted container storage pools in a cloud environment. If you specify a password for database backup, you must specify the same password on the RESTORE DB command to restore the database. You must use a password if you specify the RESTOREKEYS=YES or RESTOREKEYS=ONLY parameter.

Example: Restore the database to its most current state

Restore the database to its most current state by using the already configured active log directory.

```
dsmserv restore db
```

Example: Restore the server master key without restoring the database

Restore the server master key without restoring the database by issuing the following command:

```
dsmserv restore db restorekeys=only
```

DSMSERV RESTORE DB (Restore a database to a point-in-time)

Use this command to restore a database to a point in time. A volume history file and a device configuration file must be available.

Restriction: You cannot restore a server database if the release level of the server database backup is different from the release level of the server that is being restored. For example, an error occurs when you restore a Version 7.1.3 database and you are using a Version 8.1 IBM Spectrum Protect™ server.

You can use full and incremental database backups, or snapshot database backups can be used to restore a database to a point in time.

Tip: When you restore a V7 or later IBM Spectrum Protect server database to a specific point in time, the preferred method is to issue the DSMSERV REMOVE DB command before you issue the DSMSERV RESTORE DB command. This ensures that the system is in a clean state. The system drops and uncatalogs the database in the background. When you restore data to a specific point in time, all the required logs and the database image are retrieved from the backup media.

Syntax

```
>>-DSMSERV -+----------------------+---------------------------->
            |  (1)                 |
            '------- -u--user_name-'

                                (2).- -k--Server1--.
>--+-------------------------+------+---------------+----------->
   |  (1)                    |      '- -k--key_name-'
   '------- -i--instance_dir-'

>--+-------------------+--+---------------+--RESTORE DB--------->
   '- -o--options_file-'  |  (1)          |
                          '------- -quiet-'

                    .-TOTime--=--23:59:59-.
>--TODate--=--date--+---------------------+--------------------->
                    '-TOTime--=--time-----'

   .-Source--=--DBBackup-------.
>--+-----------------------------+------------------------------->
   '-Source--=--+-DBBackup---+-'
                '-DBSnapshot-'

>--+---------------------------+------------------------------->
   '-RECOVerydir--=--directory-'

>--+---------------------------+------------------------------->
   '-ACTIVELOGDir--=--directory-'

                                    .-PReview--=--No------.
>--+--------------------------------+--+--------------------+---->
   '-ON--=--target_directory_file-'  '-PReview--=--+-Yes-+-'
                                                   '-No--'

   .-RESTOREKeys--=--No-------.
>--+--------------------------+------------------------------->
   '-RESTOREKeys--=--+-No---+-'
                     +-YES--+
                     '-ONLY-'

>--+---------------------------+------------------------------><
   '-PASSword--=--password_name-'
```

Notes:

1. This parameter applies to only AIX® and Linux servers.
2. This parameter applies only to Windows servers.

Parameters

AIX Linux -u user_name

AIX Linux Specifies a user name to switch to before you initialize the server.

AIX Linux -i instance_dir

AIX Linux Specifies an instance directory to use. This becomes the current working directory of the server.

Windows -k key_name

Windows Specifies the name of the Windows registry key from which to retrieve information about the server. The default is SERVER1.

-o options_file
Specifies an options file to use.

AIX Linux -quiet
AIX Linux Specifies that messages to the console are suppressed.

TODate (Required)
Specifies the date to which to restore the database. The following values are possible:

MM/DD/YYYY
Specifies that you want to restore a database by using the last backup series that was created before this specified date.

TODAY
Specifies that you want to restore a database by using the most recent backup series that was created before today.

TODAY-numdays or -numdays
Specifies that you want to restore a database by using the most recent backup series that was created the specified number of days before the current date.

TOTime
Specifies the time of day to which to restore the database. This parameter is optional. The default is the end of the day (23:59:59). Possible values are:

HH:MM:SS
Specifies that you want to restore the database by using the last backup series that is created on or before the specified time on the date that is specified on the TODATE parameter.

NOW
Specifies that you want to restore the database by using a backup series that is created on or before the current time on the date that is specified on the TODATE parameter.

For example, if you issue the DSMSERV RESTORE DB utility at 9:00 with TOTIME=NOW, the database is restored by using the last backup series that is created on or before 9:00 on the date that is specified on the TODATE parameter.

NOW-numhours:numminutes or -numhours:numminutes
Specifies that you want to restore the database by using a backup series that is created on or before the current time minus a specified number of hours and, optionally, minutes on the date that is specified on the TODATE parameter.

For example, if you issue the DSMSERV RESTORE DB utility at 9:00 with TOTIME=NOW-3:30 or TOTIME+-3:30, the database is restored by using the last backup series that is created on or before 5:30 on the date that is specified on the TODATE parameter.

Source
Specifies whether the database is restored by using either database full and incremental backup volumes or snapshot database volumes. This parameter is optional. The default value is DBBackup. The following values are possible:

DBBackup
Specifies that the database is restored as follows:

1. Reads the volume history file to locate the database full and incremental backup volumes that are needed.
2. Requests mounts and loads the data from the database full and incremental backup volumes as required to restore the database volume to the specified time.

DBSnapshot
Specifies that the database is restored as follows:

1. Reads the volume history file to locate the snapshot database volumes that are needed,
2. Requests mounts and loads data from snapshot database volumes as required to restore the volume to the specified time.

RECOVerydir
Specifies a directory in which to store recovery log information from the database backup media. This log information is used to establish transaction consistency of the server database as part of the recovery processing. This directory must have enough space to hold this transaction recovery information and must be an empty directory. If this parameter is not specified, the default is the directory that is specified by one of the following parameters in the DSMSERV FORMAT or DSMSERV LOADFORMAT utility:

- ARCHFAILOVERLOGDIRECTORY, if specified
- ARCHLOGDIRECTORY, if ARCHFAILOVERLOGDIRECTORY is not specified

ACTIVELOGDir
Specifies a directory in which to store the log files that are used to track the active database operations. Specify this directory only if the intent is to switch to an active log directory that is different from the one that was already configured.

On
Specifies a file that lists the directories to which the database is restored. Specify each directory on a separate line in the file. For example, the ON parameter specifies the restorelist.txt file, which contains the following list: AIX Linux

```
/tsmdb001
/tsmdb002
/tsmdb003
```

Windows

```
e:\tsm\db001
f:\tsm\db002
g:\tsm\db003
```

If this parameter is not specified, the original directories that were recorded in the database backup are used.
Tip: If you specify multiple directories, ensure that the underlying file systems are of equal size to ensure a consistent degree of parallelism for database operations. If one or more directories for the database are smaller than the others, they reduce the potential for optimized parallel prefetching and distribution of the database.

PReview
Specifies that the volume history files be examined and that the database backup volumes from the volume history file be evaluated.

1. Which set of database backup volumes best meets the point-in-time criteria that are specified for restore processing? The volume history information provides details about the backup series ID, the operation ID (full, incremental 1, incremental 2, and so on), the date of the database backup, and the device class. This information and the parameters that are specified in the DSMSERV RESTORE DB command determine what to use to perform the restore. The volume history file is examined to find the best database backup that meets the specified point-in-time criteria and then perform the restore by using that backup.
2. Is self-describing data available for the selected set of database backup volumes? Cross-check the volume history information for this backup series. The reconciliation reports what the self-describing data contains compared to what was learned from the volume history entries. The cross-check involves mounting one or more of the volumes that are indicated by the volume history. Then, using the self-describing data that was included in the database backup volumes, that information is reconciled against what is in the volume history for the database backup. If the information from the volume history file is inconsistent with the self-describing data, then messages are issued to identify the problem. For example, not all values are specified and available, and no self-describing data is found.

If the volume history information is consistent with self-describing data from the database backup, a message is issued indicating that the database backup can be used for restore processing.

If the volume history information is inconsistent with the self-describing data from the database backup or if the self-describing data for the backup cannot be found, error messages are issued indicating what was checked and what was missing.

If the PREVIEW parameter is not specified or if it is set to NO, and if the volume history and self-describing data from the database backup are consistent, then the restore proceeds.

If the PREVIEW parameter is not specified or if it is set to NO, and the reconciliation and validation fail, the database restore is not performed. Make extra volumes available and referred to from the volume history file, or remove the incomplete backup series or operation so that the IBM Spectrum Protect server selects a different preferred series or operation and continues processing.

If the PREVIEW parameter is set to YES, the process performs only the evaluation of the volume history file and the reconciliation and validation against the selected database backup.

AIX Linux Windows RESTOREKeys
AIX Linux Windows Specifies whether to restore the server master encryption key that is used to encrypt storage pool data when the database is restored. This parameter is optional and only applies if you are using encrypted container storage pools in a cloud environment. If the server master key is protected when the database is restored, the default is YES. If the server master key is not protected when the database is restored, the default is NO. You can specify one of the following values:

No
Specifies that the server master key is not restored when the database is restored.

Yes
Specifies that the server master key is restored when the database is restored. You must specify a password with this parameter.

Only
Specifies that only the server master key is restored. The database is not restored.

AIX Linux Windows PASSword
AIX Linux Windows Specifies the password that is used to protect the database backup. This parameter only applies if you are using encrypted container storage pools in a cloud environment. If you specify a password for database backup, you must specify the same password on the RESTORE DB command to restore the database. You must use a password if you specify the RESTOREKEYS=YES or RESTOREKEYS=ONLY parameter.

Example: Restore the database to a specific point in time

Restore the database to its state on May 12, 2011 at 2:25 PM.

```
dsmserv restore db todate=05/12/2011 totime=14:45
```

Example: Restore the server master key without restoring the database

Restore the server master key without restoring the database by issuing the following command:

```
dsmserv restore db restorekeys=only
```

Windows

DSMSERV UPDATE (Create registry entries for a server instance)

Use this utility to create registry entries for an IBM Spectrum Protect™ server instance if the entries were accidentally deleted.

Run this utility from the instance directory for the database (where files such as dsmserv.dsk are stored for the server). The utility re-creates the original registry entries for the server.

Syntax

```
            .- -k--Server1--.
>>-DSMSERV--+---------------+--UPDATE-------------------------><
            '- -k--key_name-'
```

Parameters

-k key_name
Specifies the name of the Windows registry key in which to store information about the server. The default is Server1.

Example: Re-create registry entries for a server instance

Run the utility to re-create registry entries for the server instance, Server2.

```
"c:\Program Files\Tivoli\TSM\server\bin\dsmserv" -k server2 update
```

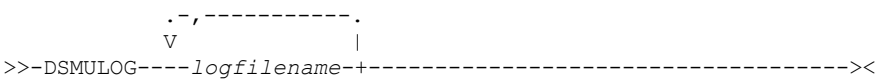
AIX Linux

DSMULOG (Capture IBM Spectrum Protect server messages to a user log file)

Use this command to capture IBM Spectrum Protect™ server console messages to a user log file. You can specify that IBM Spectrum Protect writes messages to more than one user log file.

Important: Do not place the user logs in the /usr or /opt file systems because space constraints in the file system can prevent the server from starting.

Syntax



Parameters

logfilename (Required)
: Specifies the name of one or more user log files to which IBM Spectrum Protect writes server console messages. When you specify multiple file names, each file is written to for one day and then the server moves to the next file to capture log messages. When all the files in the list have been written to, the server begins writing to the first file again and any messages contained therein are overwritten.

Example: Capture server console messages to a user log file on a daily basis

Specify the user log files to which you want to log console messages.
In this example, if you invoke this utility on Friday, on Friday the server messages are captured to log1, on Saturday the messages are captured to log2, and on Sunday the messages are captured to log3. On Monday, the messages are captured to log1 and the messages from the previous Friday are overwritten.

```
/opt/tivoli/tsm/server/bin/dsmserv -u tsminst1 -i
/tsmserv/tsminst1/tsminst1 2>&1 | dsmulog /tsmserv/tsminst1/tsminst1/log1
/tsmserv/tsminst1/tsminst1/log2
/tsmserv/tsminst1/tsminst1/log3 &
```

Утилиты устройств сервера IBM Spectrum Protect

Утилиты устройств можно использовать для задач, связанных с конфигурированием устройств хранения для сервера.

Утилиты устройств

- Операционные системы AIXdsmsanlist (Вывод информации об устройствах)
- Операционные системы Linuxautoconf (Автоматическое конфигурирование устройств)
- Операционные системы Windowstsmdlst (Вывод информации об устройствах)

Операционные системы AIX Операционные системы Linux

dsmsanlist (Вывод информации об устройствах)

Используйте утилиту информации об устройствах dsmsanlist, чтобы вывести на экран информацию об устройствах, подключенных к серверу IBM Spectrum Protect.

Утилита dsmsanlist является частью сервера IBM Spectrum Protect и пакета агента хранения IBM Spectrum Protect. Утилита устанавливается вместе с сервером IBM Spectrum Protect или агентом хранения IBM Spectrum Protect. По умолчанию утилита находится либо в каталоге server/bin (/opt/tivoli/tsm/server/bin), либо в каталоге агента хранения (/opt/tivoli/tsm/StorageAgent/bin).

Утилита dsmsanlist использует интерфейс API адаптера шины хоста (host bus adapter, HBA) для получения информации об устройствах из сети хранения данных (storage area network, SAN). Поэтому, прежде чем вы запустить утилиту, убедитесь, что у вас также установлена библиотека API поставщика HBA.

Утилиту dsmsanlist можно запустить, перейдя в соответствующий каталог (либо /opt/tivoli/tsm/server/bin, либо /opt/tivoli/tsm/StorageAgent/bin) и введя команду dsmsanlist. У этой утилиты нет никаких дополнительных опций.

Утилита dsmsanlist в качестве выходных данных покажет следующую информацию:

- Информация HBA
- Номер порта HBA
- ID поставщика устройства
- ID продукта
- Тип устройства
- Серийный номер устройства
- Имя порта по всему миру
- Имя устройства IBM Spectrum Protect

Также по умолчанию генерируется файл журнала (dsmsanlist.log), который можно использовать для отладки.
 Операционные системы AIX  Операционные системы Linux

Пример: просмотр сведений обо всех устройствах

Вызвать на экран информацию о всех устройствах, подключенных к серверу IBM Spectrum Protect:

```
dsmsanlist

root@xlinux3:/opt/tivoli/tsm/server/bin]# ./dsmsanlist

****************************************
*       IBM Spectrum Protect       *
*       Утилита dsmsanlist         *
****************************************
Лицензионные материалы - Собственность IBM

(C) Copyright IBM Corporation 2013. Все права защищены.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corporation.

Порт #1  ID_вендора   ID_продукта       Тип     Серийный_номер            WWN_порта
Имя_устройства
================================================================================================
====================
          IBM         ULTRIUM-TD8       Лента    C3EAC62000               500308c3eac62001
/dev/sg13;
          QUANTUM     Scalar i3-i6      Сменный  QUANTUMFFC1652024_LLA     500308c3eac62001
/dev/sg28;/dev/changer-sg28;
          IBM         ULTRIUM-HH7       Лента    11C1A030B5               5000e111c1a030b6
/dev/sg1;
          BDT         MULTISTAK         Сменный  DE68101026_LL01           5000e111c1a030b6
/dev/sg2;/dev/changer-sg2;
          IBM         ULTRIUM-HH6       Лента    11C1A030BF               5000e111c1a030c0
/dev/sg3;
          HPE         Ultrium 8-SCSI    Лента    9C1730D495               5001438016044f42
/dev/sg8;
          HP          1x8 G2 AUTOLDR    Сменный  4C6140X001               5001438016044f42
/dev/sg21;/dev/changer-sg21;
          IBM         ULTRIUM-TD8       Лента    C3EAC62114               500308c3eac62115
/dev/sg24;
================================================================================================
====================
```

 Операционные системы Linux

autoconf (Автоматическое конфигурирование устройств)

Утилита autoconf позволяет сконфигурировать устройства для использования с сервером IBM Spectrum Protect.

Утилита autoconf выполняет следующие задачи:

- Загружает драйвер в ядро
- Создает необходимые файлы для драйвера устройств IBM Spectrum Protect
- Создает информационные файлы устройств для библиотек и ленточных накопителей

Утилита autoconf входит в состав пакета драйверов устройств и устанавливается в каталоге /opt/tivoli/tsm/devices/bin.

Параметры

-a

Добавляет разрешения чтения и записи к файлам устройств IBM Spectrum Protect, чтобы у всех пользователей был доступ к этим устройствам. Задайте это значение для конфигурирования устройств, если сервер IBM Spectrum Protect запущен не пользователем root.

-g

Добавляет разрешения чтения и записи к файлам устройств IBM Spectrum Protect, чтобы все пользователи из группы, в которую входит пользователь root, могли использовать эти устройства.

-t

Включает трассировку для утилиты autoconf.

-?

Выводит информацию об утилите autoconf и ее параметрах.

Пример: Конфигурирование устройств при помощи утилиты autoconf

Запустите утилиту autoconf, чтобы сконфигурировать устройства IBM Spectrum Protect:

```
> /opt/tivoli/tsm/devices/bin/autoconf
```

 Операционные системы Linux

Пример: Для сервера, запущенного с использованием ID пользователя, не являющегося пользователем root, сконфигурируйте устройства при помощи утилиты autoconf

Запустите autoconf, чтобы сконфигурировать устройства IBM Spectrum Protect. Используйте опцию a, так как сервер запускается с использованием ID пользователя, не являющегося пользователем root.

```
> /opt/tivoli/tsm/devices/bin/autoconf -a

Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg4.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg5.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg6.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg7.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg8.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg9.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg10.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg11.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg12.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg13.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg14.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg15.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg16.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg17.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg18.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg19.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg20.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg21.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg22.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg23.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg24.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg25.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg26.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg27.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg28.
Добавлены разрешения на чтение и запись для всех пользователей для /dev/sg29.

Ленточные накопители
====================
Index Minor Host CHN ID  LUN Type Vendor_ID Device_Serial_Number Product_ID       Rev.
000   004   003  000 004 000 001  IBM       1068000439                ULTRIUM-HH5      C5X1
001   007   003  000 008 001 001  HP        01UbWSD-04                Ultrium 2-SCSI   R210
002   008   003  000 008 002 001  HP        01UbWSD-05                Ultrium 2-SCSI   R210
003   010   003  000 008 004 001  HP        01UbWSD-07                Ultrium 3-SCSI   R210
004   012   003  000 008 006 001  HP        01UbWSD-01                Ultrium 3-SCSI   R210
005   013   003  000 008 007 001  HP        01UbWSD-02                Ultrium 3-SCSI   R210
006   014   003  000 008 008 001  HP        01UbWSD-08                Ultrium 3-SCSI   R210
007   015   003  000 008 009 001  HP        01UbWSD-09                Ultrium 3-SCSI   R210
008   016   003  000 008 010 001  HP        01UbWSD-0a                Ultrium 3-SCSI   R210
009   017   003  000 008 011 001  HP        01UbWSD-0b                Ultrium 3-SCSI   R210
010   018   003  000 008 012 001  HP        01UbWSD-0c                Ultrium 3-SCSI   R210
011   019   003  000 008 013 001  HP        01UbWSD-0d                Ultrium 3-SCSI   R210
```

```
012   020   003  000 005 000 001  IBM       1068000913                ULTRIUM-HH5      C5X1
013   022   003  000 009 001 001  QUANTUM   01UbWSD-0f                SDLT320          R210
014   023   003  000 009 002 001  QUANTUM   01UbWSD-0g                SDLT320          R210
015   024   003  000 009 003 001  QUANTUM   01UbWSD-0h                SDLT320          R210
016   025   003  000 009 004 001  QUANTUM   01UbWSD-0i                SDLT320          R210
017   026   003  000 006 000 001  IBM       1068001573                ULTRIUM-HH4      B5Q1
018   027   003  000 007 000 001  IBM       1068001545                ULTRIUM-HH4      B5Q1
019   028   003  000 010 000 001  HP        HU19477PAE                Ultrium 5-SCSI   I65W

Устройства сменных носителей
============================
Index Minor Host CHN ID  LUN Type Vendor_ID Device_Serial_Number Product_ID       Rev.
000   005   003  000 004 001 008  NEC       2Y11BB0023                LL-2B01          0004
001   006   003  000 008 000 008  HP        01UbWSD-03                VLS              1.00
002   009   003  000 008 003 008  HP        01UbWSD-06                ThinStor AutoLdr T133
003   011   003  000 008 005 008  HP        01UbWSD-00                ESL E-Series     2.00
004   021   003  000 009 000 008  HP        01UbWSD-0e                MSL6000 Series   0430
005   029   003  000 010 001 008  HP        3615-0101                 MSL G3 Series    1120
```

Операционные системы Windows

tsmdlst (Вывод информации об устройствах)

Используйте утилиту tsmdlst, чтобы вывести на экран информацию об устройствах, подключенных к серверу IBM Spectrum Protect. Вы сможете увидеть имена устройств и другую информацию об устройстве со сменой носителей и ленточных устройствах, которые управляются драйвером устройств IBM Spectrum Protect.

Утилита tsmdlst является частью сервера IBM Spectrum Protect и пакета агента хранения IBM Spectrum Protect. По умолчанию утилита находится в каталоге установки устройств (либо C:\Program Files\Tivoli\TSM \server, либо C:\Program Files\Tivoli\TSM\StorageAgent). Утилита tsmdlst использует интерфейс API адаптера шины хоста (host bus adapter, HBA) для получения информации об устройствах из сети хранения данных (storage area network, SAN). Поэтому, прежде чем вы запустить утилиту, убедитесь, что у вас также установлена библиотека API поставщика HBA.

Утилиту можно запустить, перейдя в соответствующий каталог (либо C:\Program Files\Tivoli\TSM \server, либо C:\Program Files\Tivoli\TSM\StorageAgent) и введя команду tsmdlst.exe. У этой утилиты нет никаких дополнительных опций.

Утилита tsmdlst в качестве выходных данных покажет следующую информацию:

- Информация HBA
- Номер порта HBA
- ID поставщика устройства
- ID продукта
- Тип устройства
- Серийный номер устройства
- Имя порта по всему миру
- Имя устройства операционной системы
- Имя устройства IBM Spectrum Protect

Также по умолчанию генерируется файл журнала (tsmdlst.log), который можно использовать для отладки.

Пример: просмотр сведений об устройствах

Вывести на экран информацию об устройстве со сменой носителей и ленточных устройствах, запустив утилиту tsmdlst:

```
tsmdlst.exe

C:\Program Files\Tivoli\TSM>tsmdlst.exe
****************************************
*       IBM Spectrum Protect           *
*       Утилита SAN tsmdlst            *
****************************************
Лицензионные материалы - Собственность IBM

5608-E01
5608-E02

(C) Copyright International Business Machines Corp. 1990, 2011.
Все права защищены.
```

```
Порт #1  ID_вендора   ID_продукта       Тип     Серийный_номер              WWN_порта
Устр_ОС    Имя_устр
=============================================================================================
====================
          IBM         ULTRIUM-HH6       Лента    11C1A030BF                  5000e111c1a030c0
Tape6     mt2.0.0.5
          IBM         ULTRIUM-HH7       Лента    11C1A030B5                  5000e111c1a030b6
Tape7     mt3.0.0.5
          IBM         ULTRIUM-TD8       Лента    C3EAC62114                  500308c3eac62115
Tape8     mt0.0.0.5
          IBM         ULTRIUM-TD8       Лента    C3EAC62000                  500308c3eac62001
Tape9     mt1.0.0.5
          QUANTUM     Scalar i3-i6      Сменный  QUANTUMFFC1652024_LLA       500308c3eac62001
Changer     lb1.1.0.5
          BDT         MULTISTAK         Сменный  DE68101026_LL01             5000e111c1a030b6
Changer     lb3.1.0.5
          HPE         Ultrium 8-SCSI    Лента    9C1730D495                  5001438016044f42
Tape     mt5.0.0.5
          HP          1x8 G2 AUTOLDR    Сменный  4C6140X001                  5001438016044f42
Changer     lb5.1.0.5
=============================================================================================
====================
```

Серверные сценарии для автоматизации

Можно автоматизировать выполнение общих административных задач, создав сценарии сервера IBM Spectrum Protect или административные макрокоманды клиента. Сценарии сервера хранятся в базе данных сервера, и можно запланировать их запуск с использованием административной команды расписания. Административные макрокоманды клиента хранятся в виде файлов на административном клиенте. Макрокоманды не передаются другим серверам и их выполнение не может быть запланировано на сервере.

- Серверные сценарии
  Выполнение общих административных задач можно автоматизировать, используя сценарии, хранящиеся в базе данных сервера. Обработку сценария можно запланировать, используя планировщик административных команд на сервере.
- Макрокоманды клиента администрирования
  Макрокоманда — это файл, содержащий одну или несколько команд клиента администрирования. Выполнить макрокоманду с клиента администрирования можно только в пакетном или интерактивном режиме. Макрокоманды хранятся в виде файла в клиенте администрирования. Макрокоманды не передаются другим серверам и их выполнение не может быть запланировано на сервере.

Серверные сценарии

Выполнение общих административных задач можно автоматизировать, используя сценарии, хранящиеся в базе данных сервера. Обработку сценария можно запланировать, используя планировщик административных команд на сервере.

У сценариев IBM Spectrum Protect есть следующие возможности и операторы:

- Подстановка параметра команды.
- Команды SELECT, которые вы задаете при обработке сценария.
- Управление выполнением команд, например, опции обработки PARALLEL и SERIAL.
- Условные операторы логического потока. В число этих операторов логического потока входят следующие операторы:
  - Условие IF; это условие определяет, каким образом должна происходить обработка, исходя из текущего значения кода возврата.
  - Оператор EXIT; этот оператор завершает обработку сценария.
  - Оператор GOTO и LABEL. Этот оператор направляет логический поток для продолжения обработки со строки, начинающейся с указанной метки.
- Строки примечаний.

Примеры сценариев есть в файле scripts.smp. В примерах сценариев приведен примерный порядок выполнения для планирования выполнения команд администрирования.

Если какая-либо из указанных в сценарии команд не была успешно обработана, следующие команды не обрабатываются.

- Как задать сценарий сервера
  Чтобы создать серверный сценарий, вы можете создать его построчно, создать файл, содержащий командные строки, или скопировать существующий сценарий.
- Изменение сценария
  Сценарий можно изменить, чтобы изменить командную строку или чтобы добавить командную строку в сценарий.
- Запрос серверного сценария для создания другого серверного сценария
  Можно создать дополнительные серверные сценарии при помощи запроса сценария и указания параметров FORMAT=RAW и OUTPUTFILE. Выходные данные можно использовать как входные для другого сценария без необходимости создавать сценарий построчно.
- Запуск сценария сервера
  Чтобы обработать сценарий, введите команду RUN. Можно выполнить сценарий, содержащий переменные подстановки, задав их вместе с командой RUN.

Как задать сценарий сервера

Чтобы создать серверный сценарий, вы можете создать его построчно, создать файл, содержащий командные строки, или скопировать существующий сценарий.

Об этой задаче

Ограничение: Перенаправить вывод команды в серверном сценарии невозможно. Вместо этого запустите сценарий, а затем укажите перенаправление команды. Так, чтобы направить вывод script1 в каталог c:\temp\test.out, запустите сценарий и задайте перенаправление команды, как в следующем примере:

```
run script1 > c:\temp\test.out
```

Процедура

1. Задайте сценарий с помощью команды DEFINE SCRIPT. Используя эту команду, вы можете создать первую строку сценария. Например:

   ```
   define script qaixc "select node_name from nodes where platform='aix'"
   desc='Display AIX clients'
   ```

   В этом примере сценарий определен как QAIXC. При выполнении сценария будут показаны все клиенты AIX.
2. Задайте дополнительные строки, используя команду UPDATE SCRIPT. Например, чтобы добавить команду QUERY SESSION, введите:

   ```
   update script qaixc "query session *"
   ```

3. Необязательно: Параметр WAIT можно задать с помощью команды DEFINE CLIENTACTION. При помощи этого параметра можно указать, что действие клиента должно завершиться перед обработкой следующего действия в командном сценарии или в макрокоманде.
4. Необязательно: Чтобы вы смогли найти ошибку команды в сценарии, используйте команду ISSUE MESSAGE.

- Параллельное и последовательное выполнение команд
  Команды в сценарии могут выполняться последовательно, параллельно или и последовательно, и параллельно. Для этого используются команды сценария SERIAL или PARALLEL в параметре COMMAND_LINE DEFINE и UPDATE SCRIPT. Поэтому можно параллельно выполнить несколько команд и подождать их завершения, после чего выполнить следующую команду.
- Размещение команд на нескольких командных строках
  Можно разместить длинные команды на нескольких командных строках, указав символ продолжения (-) как последний символ в соответствующей команде.
- Как включить переменные подстановки в сценарий
  В сценарий можно включать переменные подстановки. Переменные подстановки указываются при помощи символа $, после которого вводится число, обозначающее позицию параметра при обработке сценария.
- Включение логических операторов потока в сценарий
  Можно использовать условные операторы логического потока, основанные на возвращаемых кодах, полученных после обработки предыдущей команды. При помощи этих логических операторов можно обрабатывать сценарии в соответствии с результатами некоторых команд. Можно использовать операторы IF, EXIT или GOTO (метка).
- Использование команд SELECT в сценарии
  Сценарий IBM Spectrum Protect представляет собой одну или несколько команд, которые хранятся в виде объектов базы данных. Можно задать сценарий, содержащий одну или несколько команд SELECT.

Параллельное и последовательное выполнение команд

Команды в сценарии могут выполняться последовательно, параллельно или и последовательно, и параллельно. Для этого используются команды сценария SERIAL или PARALLEL в параметре COMMAND_LINE DEFINE и UPDATE SCRIPT. Поэтому можно параллельно выполнить несколько команд и подождать их завершения, после чего выполнить следующую команду.

Об этой задаче

Последовательное выполнение команд гарантирует, что все предшествующие команды будут завершены перед запуском текущей и что все последующие команды будут запускаться последовательно. При запуске сценария все команды выполняются последовательно, пока не встретится команда PARALLEL. Несколько команд, выполняющихся в параллельном режиме и обращающихся к общим ресурсам, таким как, ленточные накопители, могут выполняться последовательно.

Коды возврата сценария остаются без изменений и до, и после выполнения команды PARALLEL. Если встречается команда SERIAL, возвращаемый сценарием код - это максимальный из кодов возврата любых команд, ранее выполнявшихся параллельно.

Если после команды PARALLEL выполняются команды сервера, поддерживающие параметр WAIT, то схема действий выглядит следующим образом:

- Если указан (или используется по умолчанию) параметр WAIT=NO, встретив следующую команду SERIAL, сценарий не будет ожидать завершения команды. Код возврата команды будет отражать обработку только до момента запуска командой фонового процесса. Завершающий код возврата команды недоступен вашему сценарию.
- Если задать параметр WAIT=YES, встретив следующую команду SERIAL, сценарий будет ожидать завершения команды. Код возврата команды будет отражать обработку всей команды.

В большинстве случаев для команд, выполняемых параллельно, можно использовать вариант WAIT=YES.

Ограничение: Если команда запускает фоновый процесс, для которого не задан параметр WAIT, то команда считается выполненной после запуска фонового потока. Поэтому команда может выполняться только в параллельном режиме.

В следующем примере показано использование команды PARALLEL для резервного копирования, переноса и восстановления пулов хранения.

```
/*выполнение параллельно нескольких команд и ожидание
их завершения перед продолжением*/
PARALLEL
/*создание резервной копии четырех пулов хранения одновременно*/
BACKUP STGPOOL PRIMPOOL1 COPYPOOL1 WAIT=YES
BACKUP STGPOOL PRIMPOOL2 COPYPOOL2 WAIT=YES
BACKUP STGPOOL PRIMPOOL3 COPYPOOL3 WAIT=YES
BACKUP STGPOOL PRIMPOOL4 COPYPOOL4 WAIT=YES
/*ожидание завершения выполнения всех предыдущих команд*/
SERIAL
/*перенос макрокоманды STGPOOLS после завершения создания резервной копии
*/
PARALLEL
MIGRATE STGPOOL PRIMPOOL1 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL2 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL3 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL4 DURATION=90 WAIT=YES
/*ожидание завершения выполнения всех предыдущих команд*/
SERIAL
/*после завершения переноса происходит одновременное восстановление
пулов хранения*/
PARALLEL
RECLAIM STGPOOL PRIMPOOL1 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL2 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL3 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL4 DURATION=120 WAIT=YES
```

Ссылки, связанные с данной:
DEFINE SCRIPT (Задать сценарий сервера)
UPDATE SCRIPT (Обновить сценарий сервера)

Размещение команд на нескольких командных строках

Можно разместить длинные команды на нескольких командных строках, указав символ продолжения (-) как последний символ в соответствующей команде.

Об этой задаче

В следующем примере оператор SQL приводится в нескольких командных строках:

```
/*-----------------------------*/
/* Пример продления */
SELECT-
* FROM-
NODE WHERE-
PLATFORM='win32'
```

При обработке команды выполняется следующее:

```
select * from nodes where platform='win32'
```

Как включить переменные подстановки в сценарий

В сценарий можно включать переменные подстановки. Переменные подстановки указываются при помощи символа $, после которого вводится число, обозначающее позицию параметра при обработке сценария.

Об этой задаче

В экземпляре сценария SQLSAMPLE указаны переменные подстановки $1 и $2:

```
/*---------------------------------------------*/
/* Пример подстановки */
/* ---------------------------------------------*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'
```

Для выполнения сценария необходимо задать два значения — для $1 и $2. Например:

```
run sqlsample node_name aix
```

При обработке сценария SQLSAMPLE выполняется следующая команда:

```
select node_name from nodes where platform='aix'
```

Включение логических операторов потока в сценарий

Можно использовать условные операторы логического потока, основанные на возвращаемых кодах, полученных после обработки предыдущей команды. При помощи этих логических операторов можно обрабатывать сценарии в соответствии с результатами некоторых команд. Можно использовать операторы IF, EXIT или GOTO (метка).

Поскольку каждая команда обрабатывается в рамках сценария, возвращаемый код сохраняется для возможной оценки до начала обработки следующей команды. Возвращаемый код может иметь один из трех уровней серьезности: OK, ПРЕДУПРЕЖДЕНИЕ или ОШИБКА. Список действительных кодов возврата и уровней серьезности смотрите в разделе Коды возврата для использования в сценариях.

- Указание оператора IF
  Оператор IF можно использовать в начале командной строки для определения способа обработки сценария, основываясь на текущем значении возвращаемого кода. В операторе IF необходимо указать символьное значение или уровень серьезности возвращаемого кода.
- Как задать оператор EXIT
  Используйте оператор EXIT, чтобы завершить обработку сценария.
- Как задать оператор GOTO
  Оператор GOTO используется вместе с оператором метки. Оператор метки является назначением оператора GOTO.

Оператор GOTO направляет процесс обработки сценария к строке, содержащей оператор метки, чтобы продолжить обработку с этого места.

Указание оператора IF

Оператор IF можно использовать в начале командной строки для определения способа обработки сценария, основываясь на текущем значении возвращаемого кода. В операторе IF необходимо указать символьное значение или уровень серьезности возвращаемого кода.

Об этой задаче

Изначально сервер задает возвращаемый код в начале сценария как RC_OK. Возвращаемый код обновляется каждой обрабатываемой командой. Если текущий возвращаемый код обрабатываемой команды соответствует какому-либо из возвращаемых кодов или уровню серьезности ошибки в операторе IF, строка обрабатывается дальше. Если текущий возвращаемый код не соответствует указанным значениям, строка пропускается.

В следующем примере сценария резервная копия пула хранения BACKUPPOOL будет создана, только если в этот момент ни один сеанс не получил доступ к серверу. Резервное копирование выполняется, только если получен возвращаемый код RC_NOTFOUND:

```
/* Резервная копия пулов хранения будет создана, если клиенты не подключены к серверу */
select * from sessions
/* Сеансы отсутствуют, если получено rc_notfound */
if(rc_notfound) backup stg backuppool copypool
```

В следующем примере сценария создается резервная копия пула хранения BACKUPPOOL, если обнаружен возвращаемый код с уровнем серьезности "предупреждение":

```
/* Резервная копия пулов хранения будет создана, если клиенты не подключены к серверу */
select * from sessions
/* Сеансы отсутствуют, если получено rc_notfound */
if(warning) backup stg backuppool copypool
```

Как задать оператор EXIT

Используйте оператор EXIT, чтобы завершить обработку сценария.

Об этой задаче

В следующем примере оператор IF используется вместе с RC_OK для определения, подключены ли клиенты к серверу. Получение возвращаемого кода RC_OK означает, что сеансы клиентов получают доступ к серверу. Выполняется оператор exit, а резервное копирование не выполняется.

```
/* Резервная копия пулов хранения будет создана, если клиенты не подключены к серверу */
select * from sessions
/* Сеансы существуют, если получено rc_ok */
if(rc_ok) exit
backup stg backuppool copypool
```

Как задать оператор GOTO

Оператор GOTO используется вместе с оператором метки. Оператор метки является назначением оператора GOTO. Оператор GOTO направляет процесс обработки сценария к строке, содержащей оператор метки, чтобы продолжить обработку с этого места.

Об этой задаче

После оператора метки всегда вводится двоеточие (:), после которого может быть пустое место. В следующем примере оператор GOTO используется для создания резервной копии пула хранения, только если в этот момент ни один сеанс не подключен к серверу. В данном примере возвращаемый код RC_OK означает, что клиенты подключены к серверу. Оператор GOTO направляет процесс обработки к метке `готово:`, которая содержит оператор EXIT, завершающий обработку сценария:

```
/* Резервная копия пулов хранения будет создана, если клиенты не подключены
к серверу */
select * from sessions
/* Сеансы существуют, если получено rc_ok */
if(rc_ok) goto done
backup stg backuppool copypool
готово:exit
```

Использование команд SELECT в сценарии

Сценарий IBM Spectrum Protect представляет собой одну или несколько команд, которые хранятся в виде объектов базы данных. Можно задать сценарий, содержащий одну или несколько команд SELECT.

Об этой задаче

Сценарий можно запустить из клиента администрирования или с серверной консоли. Его также можно включить в расписание выполнения административных команд для автоматического выполнения. Дополнительные сведения смотрите в разделе Серверные сценарии.

В состав IBM Spectrum Protect входит файл с несколькими примерами сценариев. Этот файл, scripts.smp, находится в каталоге сервера. Чтобы создавать и хранить сценарии как объекты в базе данных сервера, введите во время установки команду DSMSERV RUNFILE:

```
> dsmserv runfile scripts.smp
```

Файл можно также запустить как макрокоманду из командной строки клиента администрирования:

```
macro scripts.smp
```

Пример файла сценария содержит команды. Эти команды сначала удаляют любые сценарии с именами, подобными определенным, а затем определяют сценарии. В большинстве примеров создаются команды SELECT, но в других выполняются такие действия, резервное копирование пулов хранения. Примеры файлов сценариев можно также копировать и изменять, создавая собственные сценарии.

Ниже приводятся некоторые примеры из файла с примерами сценариев:

```
def script q_inactive_days '/* ------------------------------------------*/'
upd script q_inactive_days '/* Имя сценария:  Q_INACTIVE                 */'
upd script q_inactive_days '/* Описание: Просмотреть узлы, которые не     */'
upd script q_inactive_days '/* обращались к серверу разервного копирования */'
upd script q_inactive_days '/*  в течение заданного числа дней           */'
upd script q_inactive_days '/* Параметр 1: число дней                    */'
upd script q_inactive_days '/* Пример:     run q_inactive_days 5         */'
upd script q_inactive_days '/* ------------------------------------------*/'
upd script q_inactive_days "select node_name,lastacc_time from nodes where -"
upd script q_inactive_days " cast((current_timestamp-lastacc_time)days as -"
upd script q_inactive_days " decimal) >= $1 "

/* Просмотреть сообщения журнала операций с серьезностью X или Y       */

def script q_msg_sev desc='Просмотреть сообщ. журн. операций с серьезн. X или Y'
upd script q_msg_sev '/* ------------------------------------------------*/'
upd script q_msg_sev '/* Имя сценария:  Q_MSG_SEV                        */'
upd script q_msg_sev '/* Описание: Просмотреть сообщения в журнале       */'
upd script q_msg_sev '/*           операций с одним из двух указанных    */'
upd script q_msg_sev '/*           уровней серьезности.       */'
upd script q_msg_sev '/* Параметр 1: серьезность 1                       */'
upd script q_msg_sev '/* Параметр 2: серьезность 2                       */'
upd script q_msg_sev '/*  где серьезность - это I, W, E, S или D         */'
upd script q_msg_sev '/* Пример:  run q_msg_sev S E                      */'
upd script q_msg_sev '/* ------------------------------------------------*/'
upd script q_msg_sev "select date_time,msgno,message from actlog -"
upd script q_msg_sev "  where severity=upper('$1') or severity=upper('$2')"
```

Изменение сценария

Сценарий можно изменить, чтобы изменить командную строку или чтобы добавить командную строку в сценарий.

- Присоединение новой команды
  Чтобы добавить командную строку в конце существующего сценария, введите команду UPDATE SCRIPT без параметра LINE=. Добавленной в конце командной строке присваивается номер строки, на пять единиц больше номера последней командной строки в последовательности командных строк. Например, если сценарий заканчивается строкой 010, добавленной в конце командной строке будет присвоен номер 015.
- Замена существующей команды
  Вы можете заменить существующую строку команды, задав параметр LINE=.
- Добавление команды и номера строки
  Вы можете изменить существующий сценарий, добавив в него новые строки.
- Удаление команды из серверного сценария
  Из сценария можно удалить отдельную строку команды. Если указывается номер строки, то из сценария удаляется только соответствующая строка команды.

Присоединение новой команды

Чтобы добавить командную строку в конце существующего сценария, введите команду UPDATE SCRIPT без параметра LINE=. Добавленной в конце командной строке присваивается номер строки, на пять единиц больше номера последней командной строки в последовательности командных строк. Например, если сценарий заканчивается строкой 010, добавленной в конце командной строке будет присвоен номер 015.

Об этой задаче

Ниже приведен пример сценария QSTATUS. Сценарий содержит строки 001, 005 и 010:

```
001 /* Это сценарий QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
```

Чтобы добавить в конце сценария команду QUERY SESSION, введите следующую команду:

```
update script qstatus "query session"
```

Команде QUERY SESSION присвоен номер командной строки 015 и обновленный сценарий выглядит таким образом:

```
001 /* Это сценарий QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION
```

Замена существующей команды

Вы можете заменить существующую строку команды, задав параметр LINE=.

Об этой задаче

Строка номер 010 в сценарии QSTATUS содержит команду QUERY PROCESS. Чтобы заменить команду QUERY PROCESS на команду QUERY STGPOOL, задайте параметр LINE= следующим образом:

```
update script qstatus "query stgpool" line=10
```

В сценарий QSTATUS добавляются следующие строки:

```
001 /* Это сценарий QSTATUS */
005 QUERY STATUS
010 QUERY STGPOOL
015 QUERY SESSION
```

Добавление команды и номера строки

Вы можете изменить существующий сценарий, добавив в него новые строки.

Об этой задаче

Чтобы добавить команду QUERY NODE как новую строку 007 в сценарий QSTATUS, введите следующую команду:

```
update script qstatus "query node" line=7
```

В сценарий QSTATUS добавляются следующие строки:

```
001 /* Это сценарий QSTATUS */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION
```

Удаление команды из серверного сценария

Из сценария можно удалить отдельную строку команды. Если указывается номер строки, то из сценария удаляется только соответствующая строка команды.

Об этой задаче

Например, чтобы удалить строку команды 007 из сценария QSTATUS, введите следующую команду:

```
delete script qstatus line=7
```

Запрос серверного сценария для создания другого серверного сценария

Можно создать дополнительные серверные сценарии при помощи запроса сценария и указания параметров FORMAT=RAW и OUTPUTFILE. Выходные данные можно использовать как входные для другого сценария без необходимости создавать сценарий построчно.

Об этой задаче

В следующем примере показано, как запросить информацию из сценария SRTL2 и перенаправить вывод в newscript.script:

```
query script srtl2 format=raw outputfile=newscript.script
```

После этого вы можете изменить сценарий newscript.script при помощи редактора, имеющегося на вашем компьютере. Чтобы создать новый сценарий с использованием отредактированной выходной информации вашего запроса, введите:

```
define script srtnew file=newscript.script
```

Запуск сценария сервера

Чтобы обработать сценарий, введите команду RUN. Можно выполнить сценарий, содержащий переменные подстановки, задав их вместе с командой RUN.

Об этой задаче

Чтобы остановить выполняющийся сценарий, администратор должен остановить работу сервера. Отменить сценарий командой IBM Spectrum Protect после его запуска невозможно.

Процедура

- Произведите предварительный просмотр команд в сценарии, чтобы оценить сценарий перед его запуском. Чтобы предварительно просмотреть сценарий, не выполняя команды, введите команду RUN с параметром PREVIEW=YES. Если сценарий содержит переменные подстановки, команды будут показаны с подставленными переменными.
- Запустите сценарий, у которого нет переменных, введя следующую команду: `run qaixc`, где `qaixc` - это имя сценария.
- Запустите сценарий, содержащий переменные подстановки, задав значения переменных вместе с командой. Содержимое сценария:

```
/*---------------------------------------------*/
/* Пример продления и подстановки */
/* ---------------------------------------------*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'
```

Для выполнения этого сценария введите следующую команду:

```
run qaixc node_name aix
```

Где `имя_узла` - это значение переменной $1, а `aix` - это значение переменной $2.

Ссылки, связанные с данной:
RUN (Запустить сценарий сервера)

Макрокоманды клиента администрирования

Макрокоманда — это файл, содержащий одну или несколько команд клиента администрирования. Выполнить макрокоманду с клиента администрирования можно только в пакетном или интерактивном режиме. Макрокоманды хранятся в виде файла в клиенте администрирования. Макрокоманды не передаются другим серверам и их выполнение не может быть запланировано на сервере.

Макрокоманды могут включать следующие элементы:

- Административные команды сервера
- Замечания
- Символы продолжения
- Переменные

Имя макрокоманды должно соответствовать правилам именования клиента администрирования, выполняемого в операционной системе.

В макрокоманде, содержащей несколько команд, используйте команды COMMIT и ROLLBACK, чтобы контролировать обработку команд в макрокоманде.

Команду MACRO можно включить в файл макрокоманды, чтобы вызывать другие макрокоманды, доходя до 10 уровней вложения. Макрокоманда, вызванная из командной строки клиента администрирования, называется высокоуровневой макрокомандой. Все макрокоманды, вызванные из макрокоманды высшего уровня, называются *вложенными*.

- Запись команд в макрокоманде
  Добавьте в макрокоманду административные команды. Клиент администрирования игнорирует пустые строки в макрокоманде. Тем не менее, пустая строка приводит к остановке выполнения команды, которая продолжается (с символом продолжения).
- Добавление комментариев в макрокоманде
  Добавьте комментарии в файл макрокоманды, чтобы описать, для чего предназначена команда.
- Включение в макрокоманду символов продолжения
  В файле макрокоманды можно использовать символы продолжения, если необходимо выполнить команду, длина которой больше ширины экрана или окна.
- Как включить переменные подстановки в макрокоманде
  Переменные подстановки можно использовать в макрокоманде, чтобы при запуске макрокоманды вы смогли задать значения элементов, например, параметры команды. Если в макрокоманде применяются переменные подстановки, его можно использовать снова и снова, когда вам понадобится выполнить такую же задачу с другими объектами или с другими значениями параметров.
- Выполнение макрокоманды
  Чтобы выполнить макрокоманду, используйте команду MACRO. Команду MACRO можно ввести в пакетном или интерактивном режиме.
- Обработка команд в макрокоманде
  Если ввести команду MACRO, сервер обработает все команды в файле макрокоманды по порядку, включая команды во всех вложенных макрокомандах. Сервер выполняет все команды в макрокоманде после успешного завершения обработки макрокоманды высшего уровня.

Запись команд в макрокоманде

Добавьте в макрокоманду административные команды. Клиент администрирования игнорирует пустые строки в макрокоманде. Тем не менее, пустая строка приводит к остановке выполнения команды, которая продолжается (с символом продолжения).

Об этой задаче

Ниже приведен пример макрокоманды с именем REG.MAC, которая регистрирует и предоставляет полномочия новому администратору:

```
register admin pease mypasswd -
  contact='david pease, x1234'
grant authority pease -
  classes=policy,storage -
  domains=domain1,domain2 -
  stgpools=stgpool1,stgpool2
```

В этом примере в файле макрокоманды использованы символы продолжения. Дополнительные сведения о символах продолжения смотрите в разделе Включение в макрокоманду символов продолжения.

Когда файл макрокоманды создан, можно обновить данные, которые он содержит, и использовать его еще раз. Можно также скопировать файл макрокоманды. После копирования макрокоманды можно изменить и запустить копию.

Добавление комментариев в макрокоманде

Добавьте комментарии в файл макрокоманды, чтобы описать, для чего предназначена команда.

Об этой задаче

Чтобы добавить комментарий:

- Поставьте косую черту и звездочку (/*), чтобы обозначить начало комментария.
- Введите текст комментария.
- Введите звездочку и косую черту (*/), чтобы обозначить конец комментария.

Комментарий можно разместить в отдельной строке или в строке, которая содержит команду или часть команды.

Например, чтобы использовать примечание для указания назначения макрокоманды, введите следующую строку:

```
/* auth.mac-регистрация новых узлов  */
```

Чтобы добавить примечание, содержащее сведения о команде или части команды, введите:

```
domain=domain1             /*назначение узла для domain1  */
```

Комментарии не могут быть вложенными и не должны занимать несколько строк. Каждая строка комментария должна содержать разделители комментариев.

Включение в макрокоманду символов продолжения

В файле макрокоманды можно использовать символы продолжения, если необходимо выполнить команду, длина которой больше ширины экрана или окна.

Об этой задаче

Без символов продолжения строки можно вводить до 256 символов. С символами продолжения можно ввести до 1500 символов. В команде MACRO значения переменных подстановки включаются в число символов.

Чтобы применить символ продолжения, введите тире или обратную косую черту в конце строки, которую необходимо продлить. С помощью символов продолжения можно продолжить следующие строки в макрокоманде.

Примеры

- Продолжайте команду, например:

```
register admin pease mypasswd -
contact="david, ext1234"
```

- Продолжите список значений, введя тире или обратную косую черту без пробелов после последней запятой списка, введенного в первой строке. После этого введите оставшиеся элементы списка в следующей строке без пробела перед ними. В следующем примере список имен пулов хранения продолжается после первой строки:

  ```
  stgpools=stg1,stg2,stg3,-
  stg4,stg5,stg6
  ```

- Продолжить строку значений в кавычках, введя первую часть строки в кавычках, после чего поставьте косую черту или обратную косую черту в конце строки. Затем введите оставшуюся часть строки в следующей строке. Заключите оставшуюся часть строки в те же кавычки. В следующем примере показана строка, которая продолжается после первой строчки:

  ```
  contact="david pease, bldg. 100, room 2b, san jose,"-
  "ext. 1234, alternate contact-norm pass,ext 2345"
  ```

  Две строки объединяются путем конкатенации без пробелов между ними. Для продления строки значений в кавычках больше чем на одну строку следует использовать только этот метод.

Как включить переменные подстановки в макрокоманде

Переменные подстановки можно использовать в макрокоманде, чтобы при запуске макрокоманды вы смогли задать значения элементов, например, параметры команды. Если в макрокоманде применяются переменные подстановки, его можно использовать снова и снова, когда вам понадобится выполнить такую же задачу с другими объектами или с другими значениями параметров.

Об этой задаче

Переменная подстановки состоит из символа процента (%), после которого идет уникальное число, указывающее переменную подстановки. При выполнении файла с командой MACRO нужно указать значения для переменных.

ограничения:

- Если система использует символ процента как символ подстановки, клиент администрирования интерпретирует выражения, соответствующие шаблону, в которых после символа процента следует число, как переменную подстановки.
- Нельзя вводить переменную подстановки в кавычках. Тем не менее, значение, указанное в качестве подстановки для переменной, может быть строкой в кавычках.

Пример

Создайте макрокоманду AUTH.MAC для регистрации новых узлов. У макрокоманды есть четыре переменные подстановки для параметров в команде:

```
/* регистрация новых узлов */
register node %1 %2 -      /*  ID пользователя пароль           */
  contact=%3 -             /* 'ФИО, номер телефона'             */
  domain=%4                /*  домен политики                    */
```

При выполнении макрокоманды следует ввести значения, которые необходимо передать серверу для обработки команды.

Например, чтобы использовать макрокоманду для регистрации узла с именем DAVID, паролем DAVIDPW, включить его имя и номер телефона как контактные сведения и назначить его домену политики DOMAIN1, введите следующую команду:

```
macro auth.mac david davidpw "david pease, x1234" domain1
```

Выполнение макрокоманды

Чтобы выполнить макрокоманду, используйте команду MACRO. Команду MACRO можно ввести в пакетном или интерактивном режиме.

Об этой задаче

Если макрокоманда не содержит переменных подстановки, выполните макрокоманду, введя команду MACRO с именем файла макрокоманды. Например:

```
macro reg.mac
```

Если макрокоманда содержит переменные подстановки, включите значения, которые необходимо предоставить, после имени макрокоманды. Значения разделяются пробелами. Например:

```
macro auth.mac pease mypasswd "david pease, x1234" domain1
```

Если ввести меньше значений, чем указано переменных подстановки в макрокоманде, клиент администрирования заменит оставшиеся переменные нулевыми значениями.

Если необходимо пропустить одно или несколько значений, введите нулевую строку ("") вместо каждого пропущенного значения. Например, если пропустить контактные сведения в предыдущем примере, следует ввести:

```
macro auth.mac pease mypasswd "" domain1
```

Ссылки, связанные с данной:
MACRO (Запустить макрокоманду)

Обработка команд в макрокоманде

Если ввести команду MACRO, сервер обработает все команды в файле макрокоманды по порядку, включая команды во всех вложенных макрокомандах. Сервер выполняет все команды в макрокоманде после успешного завершения обработки макрокоманды высшего уровня.

Если в какой-либо команде макрокоманды или вложенной макрокоманды возникает ошибка, то сервер останавливает обработку и выполняет откат всех изменений, внесенных при выполнении предыдущих команд.

Если при вводе команды DSMADMC указана опция ITEMCOMMIT, сервер принимает каждую команду в сценарии или в макрокоманде по отдельности после успешного завершения обработки каждой команды. В случае возникновения ошибки сервер продолжает обработку и выполняет откат только тех изменений, которые были внесены в результате выполнения определенной команды.

С помощью команды COMMIT можно отслеживать выполнение команд. Если во время обработки сервером команды в макрокоманде происходит ошибка, то сервер останавливает обработку макрокоманды и выполняет откат всех непринятых изменений. Непринятые изменения - это команды, обработанные с момента последней команды COMMIT. Убедитесь, что ваш сеанс клиента администрирования не выполняется с опцией ITEMCOMMIT, если обработку команд следует контролировать при помощи команды COMMIT.

Вы можете проверить макрокоманду перед ее применением с помощью команды ROLLBACK. Можно ввести команды (кроме команды COMMIT), которые будут использованы в макрокоманде, и последней ввести команду ROLLBACK. После этого можно выполнить макрокоманду, чтобы убедиться, что все команды успешно обрабатываются. Любые изменения в базе данных, выполненные командами, будут отменены командой ROLLBACK. Не забудьте удалить команду ROLLBACK перед началом использования макрокоманды. Убедитесь, что ваш сеанс клиента администрирования не выполняется с опцией ITEMCOMMIT, если обработку команд следует контролировать при помощи команды ROLLBACK.

Совет: Команды, запускающие фоновые процессы, нельзя отменить.
При наличии последовательности команд, которая выполняется из командной строки, но не работает в макрокомандее, возможно, между командами есть зависимости. Возможно также, команда, введенная в макрокоманде, не может быть успешно обработана, пока не будет принята предыдущая команда, введенная в этой же макрокоманде. Любое из этих действий позволяет успешно обрабатывать эти команды в макрокоманде:

- Вставьте команду COMMIT перед командой, зависимой от предыдущей команды. Например, если COMMAND C зависит от COMMAND B, вставьте команду COMMIT перед командой COMMAND C.

  ```
  command a
  command b
  commit
  command c/
  ```

- Запустите сеанс клиента администрирования с использованием опции ITEMCOMMIT. Благодаря этой опции каждая команда в макрокоманде будет приниматься перед обработкой следующей команды.

Ссылки, связанные с данной:
COMMIT (Управление подтверждением операций в макрокоманде)
ROLLBACK (Выполнить откат изменений, не принятых в макрокоманде)

Return codes for use in IBM Spectrum Protect scripts

You can write IBM Spectrum Protect™ scripts that use return codes to determine how script processing proceeds. The return codes can be one of three severities: OK, WARNING, ERROR.

IBM Spectrum Protect scripts use the symbolic return code for processing, not the numeric value. The administrative client displays the numeric values when a command is run. The return codes are shown in the following table.

Table 1. Return codes

Return code	Severity	Numeric value	Description
RC_OK	OK	0	The command completed successfully.
RC_UNKNOWN	ERROR	2	The command is not found; not a known command.
RC_SYNTAX	ERROR	3	The command is valid, but one or more parameters were not specified correctly.
RC_ERROR	ERROR	4	An internal server error prevented the command from successfully completing.
RC_NOMEMORY	ERROR	5	The command could not be completed because of insufficient memory on the server.
RC_NOLOG	ERROR	6	The command could not be completed because of insufficient recovery log space on the server.
RC_NODB	ERROR	7	The command could not be completed because of insufficient database space on the server.
RC_NOSTORAGE	ERROR	8	The command could not be completed because of insufficient storage space on the server.
RC_NOAUTH	ERROR	9	The command failed because the administrator is not authorized to issue the command.
RC_EXISTS	ERROR	10	The command failed because the specified object already exists on the server.
RC_NOTFOUND	WARNING	11	Returned by a QUERY or SQL SELECT command when no objects are found that match specifications.
RC_INUSE	ERROR	12	The command failed because the object to be operated upon was in use.
RC_ISREFERENCED	ERROR	13	The command failed because the object to be operated upon is still referenced by some other server construct.
RC_NOTAVAILABLE	ERROR	14	The command failed because the object to be operated upon is not available.
RC_IOERROR	ERROR	15	The command failed because an input/output (I/O) error was encountered on the server.
RC_NOTXN	ERROR	16	The command failed because a database transaction failed on the server.
RC_NOLOCK	ERROR	17	The command failed because a lock conflict was encountered in the server database.
RC_NOTHREAD	ERROR	19	The command could not be completed because of insufficient memory on the server.

Return code	Severity	Numeric value	Description
RC_LICENSE	ERROR	20	The command failed because the server is not in compliance with licensing.
RC_INVDEST	ERROR	21	The command failed because a destination value was invalid.
RC_IFILEOPEN	ERROR	22	The command failed because an input file that was needed could not be opened.
RC_OFILEOPEN	ERROR	23	The command failed because it could not open a required output file.
RC_OFILEWRITE	ERROR	24	The command failed because it could not successfully write to a required output file.
RC_INVADMIN	ERROR	25	The command failed because the administrator was not defined.
RC_SQLERROR	ERROR	26	An SQL error was encountered during a SELECT statement query.
RC_INVALIDUSE	ERROR	27	The command failed because the command is used in an invalid manner.
RC_NOTABLE	ERROR	28	The command failed because of an unknown SQL table name.
RC_FS_NOTCAP	ERROR	29	The command failed because of incompatible file space name types.
RC_INVALIDADDR	ERROR	30	The command failed because of an incorrect high-level address or low-level address.
RC_INVALIDCG	ERROR	31	The command failed because the management class does not have an archive copy group.
RC_OVERSIZE_VOL	ERROR	32	The command failed because the volume size exceeds the maximum allowed.
RC_DEFVOL_FAIL	ERROR	33	The command failed because volumes cannot be defined in RECLAMATIONTYPE=SNAPLOCK storage pools.
RC_DELVOL_FAIL	ERROR	34	The command failed because volumes cannot be deleted in RECLAMATIONTYPE=SNAPLOCK storage pools.
RC_CANCELED	WARNING	35	The command is canceled.
RC_INVPOLICY	ERROR	36	The command failed because there is an invalid definition in the policy domain.
RC_INVALIDPW	ERROR	37	The command failed because of an invalid password.
RC_UNSUPP_PARM	WARNING	38	The command failed because the command or the parameter is not supported.

Related reference:
DEFINE SCRIPT (Define an IBM Spectrum Protect script)
UPDATE SCRIPT (Update an IBM Spectrum Protect script)
RUN (Run an IBM Spectrum Protect script)

Документация по серверу в файлах PDF

Вы можете скачать файлы PDF с документацией по IBM Spectrum Protect.

Совет: Начиная с IBM® Tivoli Storage Manager версии 7.1.3, публикация *Руководство администратора* в формате PDF не предоставляется. Вместо этого набор документации был исправлен, чтобы помочь вам выполнять отдельные задачи:

- Чтобы реализовать новое решение по защите данных, смотррите раздел Решения по защите данных IBM Spectrum Protect. В руководствах по решению приводятся инструкции типа справочника, которые помогут вам спланировать, реализовать решение и управлять им.
- Либо можно использовать IBM Spectrum Protect Blueprints. Можно выполнить процедуры Blueprint, чтобы внедрить среду хранения, и использовать сценарии Blueprint, чтобы наладить процесс установки и конфигурирования. В Blueprints содержатся самые последние требования к оборудованию и программам для мелких, средних и крупных сред хранения.
- Чтобы администрировать *существующее* решение, смотрите раздел Конфигурирование серверов.

Более подробную информацию о том, как выполнить задачи по внедрению и администрированию, смотрите в файлах PDF, перечисленных в следующей таблице.

Задача	**Компоненты**	**Связи**
Узнать о понятиях продукта и решениях	• Сервер • Центр операций	Введение в решения по защите данных
Внедрение наилучшего практического решения	• Сервер • Центр операций	• Руководство по дисковому решению с одной площадкой • Руководство по дисковому решению с несколькими площадками • Руководство по решению на лентах
Установка компонентов	• Сервер • Центр операций	• AIX • Linux • Windows
Обновление компонентов	• Сервер	• AIX • Linux • Windows
Использование команд и опций	• Сервер	• AIX • Linux • Windows
Использование сообщений и кодов ошибок	• Сервер	Все операционные системы

Клиенты резервного копирования и архивирования IBM Spectrum Protect

Используйте клиент резервного копирования и архивирования IBM Spectrum Protect, чтобы сохранять копии файлов и каталогов с вашей рабочей станции или файл-сервера и хранить их на сервере IBM Spectrum Protect. Вы сможете восстановить эти копии, если оригиналы вдруг окажутся повреждены или утрачены. В зависимости от того, для чего вы сохраняете данные, вы можете либо произвести их резервное копирование, либо заархивировать их.

В этот выпуск не включена обновленная версия клиента резервного копирования и архивирования. Документацию по клиенту резервного копирования и архивирования смотрите в предыдущих выпусках.

Интерфейс прикладного программирования

Интерфейс прикладного программирования (application programming interface, API) IBM Spectrum Protect включен в пакет клиента резервного копирования и архивирования IBM Spectrum Protect. При помощи API можно защитить такие бизнес-приложения, как базы данных в среде IBM Spectrum Protect.

В этот выпуск не включена обновленная версия компонента API. Документацию по API смотрите в предыдущих выпусках.

Производительность

На производительность сервера и клиентов влияет множество факторов, включая операционные системы, аппаратные средства систем, конфигурации сетей, типы устройств хранения, а также размеры и число файлов клиентов. Взаимодействие этих факторов может может усложнить оптимизацию производительности.

В этот выпуск не включена обновленная версия компонента производительности. Документацию по производительности смотрите на сайте Версия 8.1.0.

Диагностика ошибок

Доступны процедуры по устранению неисправностей для диагностики и устранения ошибок.

В этот выпуск не включена обновленная версия компонента устранения неисправностей. Документацию по устранению ошибок смотрите на сайте Версия 8.1.0.

Messages, return codes, and error codes

Explanations and suggested actions are available for messages that are issued by IBM Spectrum Protect™ components.

- Introduction to messages
- ANS 0000-9999 messages
- API return codes
- IBM Global Security Kit return codes
  The server and client use the IBM Global Security Kit (GSKit) for SSL (Secure Sockets Layer) processing between the server and the backup-archive client. Some messages that are issued for SSL processing include GSKit return codes.
- ANE: Client events logged to the server
- ANR: Server common and platform-specific messages
- I/O error code descriptions in server messages
- Device error codes in the AIX system error log
- Troubleshooting (V8.1.0 is the most recent publication)

Introduction to messages

Messages, error codes, and return codes are issued by the IBM Spectrum Protect™ server and clients.

Messages and codes can appear on the server console, the administrative client, an operator terminal, the administrative graphical user interface, the backup-archive client, or the hierarchical storage managment client (HSM client).

IBM Spectrum Protect provides an activity log to help the administrator track server activity and monitor the system. The activity log contains messages generated by the server, and is stored in the database. The server automatically deletes messages from the activity log after they have passed the specified retention period. Any messages sent to the server console are stored in the activity log. Examples of the types of messages stored in the activity log include:

- When client sessions start or end
- When migration starts or ends
- When backed up files are expired from server storage
- Any output generated from background processes

Some messages have no explanations and are not published. The client can send statistics to the server providing information about a backup or restore. These statistics are informational messages that can be enabled or disabled to the various event logging receivers. These messages are not published.

- IBM Spectrum Protect server and client messages format
- Interpreting return code messages

Related tasks:
Using the activity log (V7.1.1)

IBM Spectrum Protect server and client messages format

IBM Spectrum Protect™ server and client messages consist of the following elements:

- A three-letter prefix. Messages have different prefixes to help you identify the IBM Spectrum Protect component that issues the message. Typically, all messages for a component have the same prefix. Sometimes a component issues messages with two or three different prefixes.

  For example, backup-archive clients issue messages with the ANS prefix. Backup-archive client events that are logged to the server have the ANE prefix. Server common and server platform-specific messages have the ANR prefix.

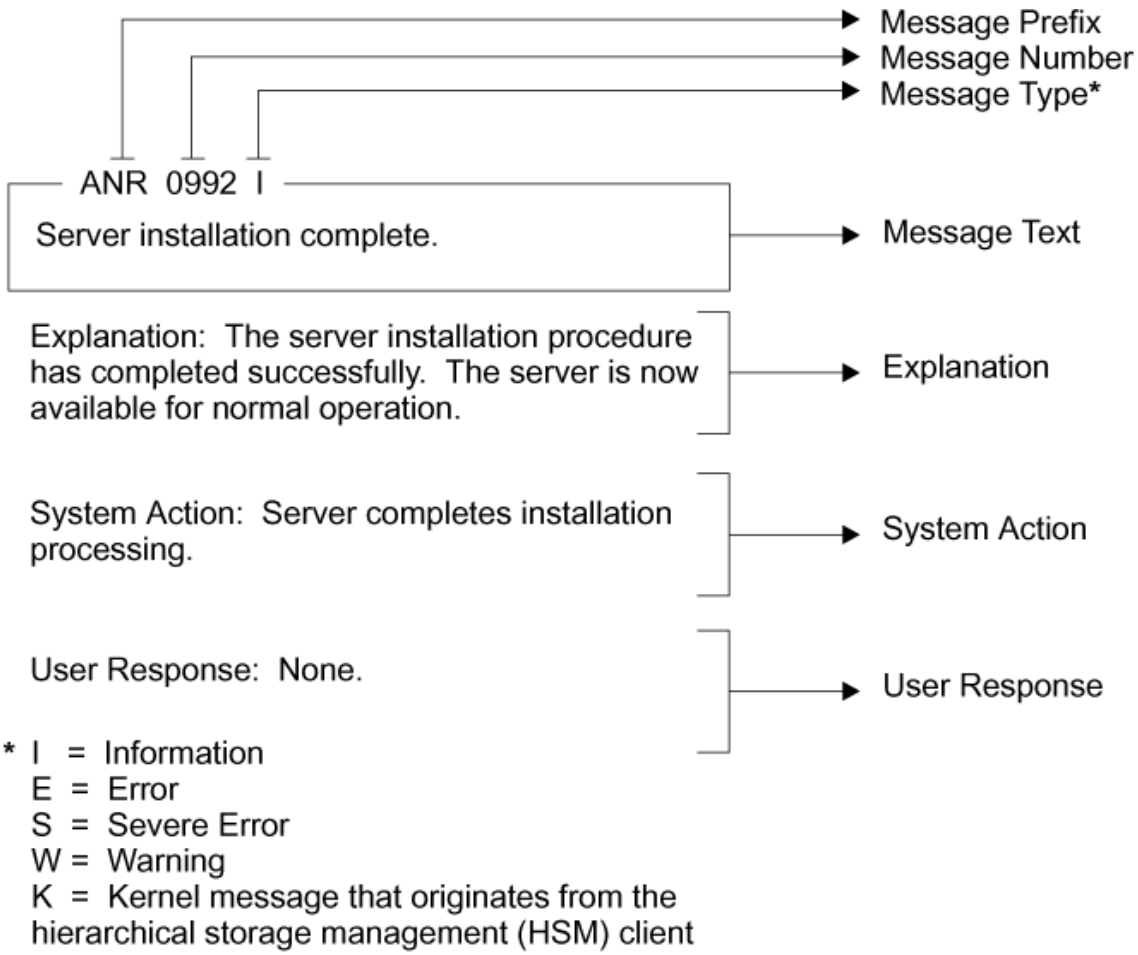
- A numeric message identifier.
- A one-letter severity code. The following codes indicate the severity of the action that generated the message:

Code	Severity	Meaning
S	Severe	The product or a product function cannot continue. User response is required.
E	Error	An error is encountered during processing. Processing might stop. User response might be required.
W	Warning	Processing continues, but problems might occur later as a result of the warning.
I	Information	Processing continues. User response is not necessary.

- Message text that is displayed on screen and written to message logs.
- Explanation, System Action, and User Response texts. These texts elaborate on the message text, and are available in the product messages publications and in the command line help.

The following image presents a typical IBM Spectrum Protect server message.

The callouts identify each element of the message.



Message variables in the message text appear in italics.

Interpreting return code messages

Many different commands can generate the same *return code*. The following examples are illustrations of two different commands issued that result in the same return code; therefore, you must read the *descriptive message* for the command.

In these examples, two different commands yield the same return code, but they also return descriptive messages that are unique to each command. The two commands are `q event standard dddd` and `def vol cstg05 primary`. Both yield a generic message with return code:

```
ANS5102I: Return Code 11.
```

But the first command also yields a descriptive message:

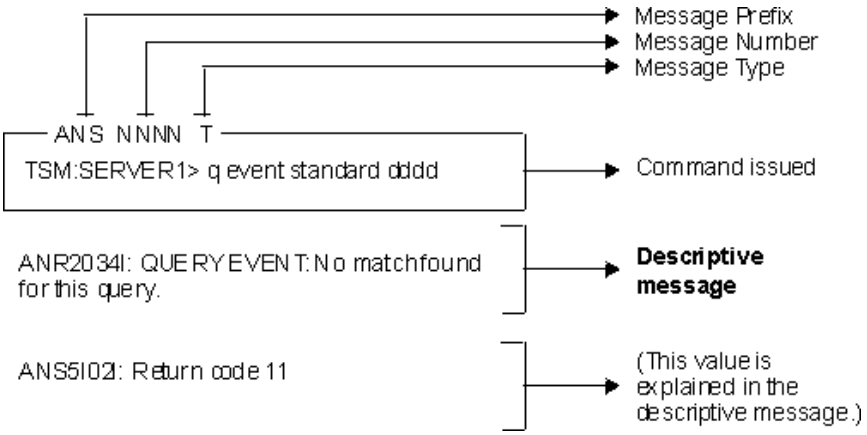
```
ANR2034I: QUERY EVENT: No match found for this query.
```

And the second command also yields a unique, descriptive message:

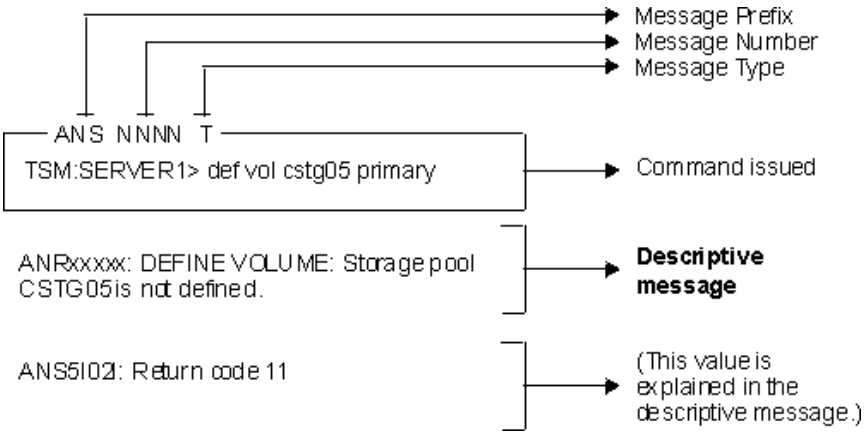
```
ANRxxxx: DEFINE VOLUME: Storage pool CSTG05 is not defined.
```

- Example one for QUERY EVENT command
- Example two for DEFINE VOLUME command

Example one for QUERY EVENT command



Example two for DEFINE VOLUME command



ANE messages

ANE messages are issued by the server. All messages with the ANE prefix are client events logged to the server.

- ANE messages list

ANR messages

ANR messages are issued by the server. Some ANR messages are common to all operating systems, and some are specific to a single operating system.

- ANR messages list

ANS 0000-9999 messages

This release does not include updated ANS-prefix messages. For documentation of ANS-prefix messages, see other releases of IBM Spectrum Protect™.

API return codes

This release does not include updated application programming interface (API) return codes. For documentation of API return codes, see other releases of IBM Spectrum Protect™.

Descriptions of I/O codes in server messages

IBM Spectrum Protect™ messages can contain input/output (I/O) codes. The codes can be operation codes, completion codes, additional sense codes (ASC), and additional sense code qualifier (ASCQ) codes.

Code descriptions are provided for I/O error messages from the IBM Spectrum Protect server for all supported operating systems.

Code

Description

OP

I/O operation that failed. These values can be displayed:

- READ
- WRITE
- FSR (forward space record)
- RSR (reverse space record)
- FSF (forward space file)
- RSF (reverse space file)
- WEOF (write end of file mark)
- OFFL (rewind and unload the tape)
- FLUSH (flush)
- GET_MEDIUM_INFO (get medium information)
- LOCATE (locate)
- QRYLBP (query logical block protection)
- RDBLKID (read block ID)
- SETLBP (set logical block protection)
- SETMODE (set mode)
- REW (rewind)
- SPACEEOD (space end of data)
- TESTREADY (test drive ready)

CC

I/O completion code. This value is returned by the device driver to the server when an error occurs. For a list of completion codes, see Completion code and operation code values overview. For information about tape library system calls and error descriptions for the library I/O control requests, see technote S7002972.

KEY

Byte 2 of the sense bytes from the error. The following lists some definitions:

0 = no additional sense bytes available
1 = recovered error
2 = not ready
3 = medium error
4 = hardware error
5 = incorrect request
6 = unit attention (for example, a SCSI bus reset)
7 = data protect

8 = blank check
9 = vendor specific
A = copy canceled
B = canceled command
C = obsolete
D = volume overflow
E = miscompare
F = reserved

ASC/ASCQ
: ASC and ASCQ codes are bytes 12 and 13 of the sense bytes. The drive or library reference manual provided with the device contains tables explaining the values of the KEY, ASC, and ASCQ fields. Descriptions of standard ASC and ASCQ codes provides additional information about standard values of ASC and ASCQ codes.

Operating system error codes
: When a command fails, the operating system returns an error number. To determine what the error codes mean, take the following action:

  - On AIX®, HP-UX, and Solaris, platforms, view the errno.h file in the /usr/include/sys directory. This file provides definitions for error codes.
  - On Linux platforms, view the errno-base.h and errno.h files in the /usr/include/asm-generic directory. These files provides definitions for codes.
  - On Windows platforms, contact Microsoft Support for help with error messages.

- Completion code and operation code values overview
  IBM Spectrum Protect messages can contain device driver completion codes from the device drivers.
- Descriptions of standard ASC and ASCQ codes
  Standard ASC and ASCQ codes are described.

Completion code and operation code values overview

IBM Spectrum Protect™ messages can contain device driver completion codes from the device drivers.

- Device drivers completion codes: Common codes
  IBM Spectrum Protect device drivers provide completion codes that are common to all device classes.
- Device drivers completion codes: Media changers
  IBM Spectrum Protect device drivers provide completion codes that are specific to media changer devices.
- Device drivers completion codes: Tape drives
  IBM Spectrum Protect device drivers provide completion codes that are specific to tape drives.

Device drivers completion codes: Common codes

IBM Spectrum Protect™ device drivers provide completion codes that are common to all device classes.

The following table shows common completion code values for IBM Spectrum Protect device drivers. Each entry provides a description for the I/O error message and the recommended action. After completing the recommended action, try the failing operation again.

Table 1. Completion code values common to all device classes

Decimal	Hexadecimal	Description	Recommended action
200	X'C8'	The device indicated a failure condition, but sense data was unavailable.	Try the failing operation again.
201	X'C9'	The device driver failed.	Contact IBM Spectrum Protect Support.
202	X'CA'	The device EEPROM failed.	Test the device. Service the device if necessary.
203	X'CB'	Manual intervention is required.	Correct the problem on the device. The problem can be a stuck tape, dirty heads, or a jammed library arm.
204	X'CC'	The system recovered from an I/O error; for your information only.	No action necessary.

Decimal	Hexadecimal	Description	Recommended action
205	X'CD'	The SCSI adapter failed.	Check for loose cables, bent pins, bad cables, bad SCSI adapters, improper termination, or bad terminators.
206	X'CE'	A general SCSI failure occurred.	Check for loose cables, bent pins, bad cables, bad SCSI adapters, improper termination, or bad terminators.
207	X'CF'	The device cannot perform the requested action.	Ensure that the device is on and ready. Ensure that the drive was defined appropriately with the DEFINE DRIVE command. Ensure that the device class was defined appropriately with the DEFINE DEVCLASS command.
208	X'D0'	The command stopped.	Contact IBM Spectrum Protect Support.
209	X'D1'	A failure is detected in the device microcode.	Check the microcode level of the drive. Contact the drive manufacturer and request the latest level.
210	X'D2'	The device was reset due to device power-up, SCSI bus reset, or manual tape load/eject.	Try the failing operation again.
211	X'D3'	The SCSI bus is busy.	Ensure that the SCSI IDs are correctly assigned to the correct device, and the device is not being accessed by another process.
212	X'D4'	Persistent reservation is not supported on this device.	No action is necessary.
213	X'D5'	A persistent reservation operation failed.	Reset the device and try the operation again. If the problem persists, contact IBM Spectrum Protect Support.

Device drivers completion codes: Media changers

IBM Spectrum Protect™ device drivers provide completion codes that are specific to media changer devices.

The following table shows completion code values for IBM Spectrum Protect device drivers for media changers. Each entry provides a description for the I/O error message and the recommended action. After performing the recommended action, try the failing operation again.

Table 1. Completion code values for media changers

Decimal	Hexadecimal	Description	Recommended action
300	X'12C'	Cartridge entry/exit error	Check the entry/exit ports for a jammed volume.
301	X'12D'	Cartridge load failure	Check the drive for jammed volumes. On AIX®, display the errpt to check for hardware errors.
302	X'12E'	Cartridge in failed drive	Check the drive for jammed volumes. On AIX, display the errpt to check for hardware errors.
303	X'12F'	Carousel not loaded	Ensure that the carousel is correctly in place and the door is shut.
304	X'130'	Changer failure	On AIX, display the errpt to check for hardware errors.

Decimal	Hexadecimal	Description	Recommended action
305	X'131'	Drive failure	Ensure that the heads are clean. On AIX, display the errpt to check for hardware errors.
306	X'132'	Drive or media failure	Ensure that the heads are clean. On AIX, display the errpt to check for hardware errors.
307	X'133'	Entry/exit failure	Check the tape library interface for hardware errors. If there are no errors, contact IBM Spectrum Protect Support.
308	X'134'	Entry/exit port not present	Check the tape library interface for hardware errors. If there are no errors, contact IBM Spectrum Protect Support.
309	X'135'	Library audit error	Ensure that there are no jammed volumes. It is possible that the library audit is failing due to hardware errors. On AIX, display the errpt to check for hardware errors.
310	X'136'	Library full	Check for jammed volumes. Ensure that the volumes are not rearranged. If the library is not full, start the AUDIT LIBRARY command.
311	X'137'	Media export	Check the tape library interface for hardware errors. If there are no errors, contact IBM Spectrum Protect Support.
312	X'138'	Slot failure	Ensure that nothing is jammed in the slot.
313	X'139'	Slot or media failure	Ensure that the volume is not jammed in the slot and that the volumes are not rearranged. If the problem persists, start the AUDIT LIBRARY command.
314	X'13A'	The source slot or drive was empty in an attempt to move a volume	Ensure that the volumes are not rearranged. If the problem persists, start the AUDIT LIBRARY command.
315	X'13B'	The destination slot or drive was full in an attempt to move a volume	Ensure that the volumes are not rearranged, or that a volume is not stuck in the drive. If problem persists, start the AUDIT LIBRARY command.
316	X'13C'	Cleaner cartridge installed	Contact IBM Spectrum Protect support.
317	X'13D'	Media not ejected	Ensure that the volumes are not rearranged, or that a volume is not stuck in the drive. If problem persists, start the AUDIT LIBRARY command.
318	X'13E'	I/O port not configured	Contact IBM Spectrum Protect Support.
319	X'13F'	First destination empty	Ensure that the volumes are not rearranged. If problem persists, start the AUDIT LIBRARY command.
320	X'140'	No inventory information	Start the AUDIT LIBRARY command.
321	X'141'	Read element status mismatch	Ensure that host bus adapter drivers and firmware are at current levels. Check the tape library interface for hardware errors. If there are no errors, contact IBM Spectrum Protect Support.

Decimal	Hexadecimal	Description	Recommended action
322	X'142'	Initialize range failed	Check the tape library interface for hardware errors. If there are no errors, contact IBM Spectrum Protect Support.

Device drivers completion codes: Tape drives

IBM Spectrum Protect™ device drivers provide completion codes that are specific to tape drives.

The following table shows completion code values for IBM Spectrum Protect device drivers for tape drives. Each entry provides a description for the I/O error message and the recommended action. After trying the recommended action, try the failing operation again.

Table 1. Completion code values for tape drives

Decimal	Hexadecimal	Description	Recommended action
400	X'190'	Physical end of media encountered	Ensure that the heads are clean on the drive.
401	X'191'	End of data detected	Contact IBM Spectrum Protect Support.
402	X'192'	Media corrupted	Ensure that the heads are clean. Ensure that the media is not physically damaged and has not reached the end of life as specified by the media manufacturer.
403	X'193'	Media failure	Ensure that the heads are clean. Ensure that the media is not physically damaged and has not reached the end of life as specified by the media manufacturer.
404	X'194'	Media incompatibility	Ensure that the correct length and type of media is being used.
406	X'196'	Sector that is requested is invalid	Internal server error. Contact IBM Spectrum Protect Support.
407	X'197'	Write protect	Ensure that the volume is not write protected.
408	X'198'	Clean the media and the drive	Clean the drive heads with a cleaning cartridge.
409	X'199'	Media fault	Ensure that the heads are clean. Ensure that the media is not physically damaged and has not reached the end of life as specified by the media manufacturer.
410	X'19A'	Cleaning complete	Try the failing operation again.
411	X'19B'	Logical end of media encountered	ContactIBM Spectrum Protect Support.
412	X'19C'	Media not present in drive	Ensure that the media is correctly positioned in the drive. If problem persists, start the AUDIT LIBRARY command.
413	X'19D'	Encountered the beginning of the media	Contact IBM Spectrum Protect Support.
414	X'19E'	Erase failure	Clean the drive heads.
415	X'19F'	Attempted to overwrite written WORM media	Internal server error. ContactIBM Spectrum Protect Support.
416	X'1A0'	An incorrect length block was read.	Ensure that the heads are clean. On AIX®, display the errpt to check for hardware errors.
417	X'1A1'	Open read only	Contact IBM Spectrum Protect Support.
418	X'1A2'	Open write only	Contact IBM Spectrum Protect Support.

Decimal	Hexadecimal	Description	Recommended action
419	X'1A2'	Media scan failed	Clean the drive and media.
420	X'1A4'	Logical write protect	Ensure that the heads are clean. Check operating system error logs for hardware errors. Verify that the write protect tab is off. Turn off SAN tape acceleration or set CHECKTAPEPOS to OFF or TSMonly.
422	X'1A6'	Cleaning is required	Clean the tape drive.
423	X'1A7'	Media error	Check operating system error logs for hardware errors. Check for bad media.
424	X'1A8'	Encryption-related error occurred	Check your encryption setting on your device class and tape drive.
425	X'1A9'	Decryption-related error occurred	Check your encryption setting on your device class and tape drive.
425	X'1AA'	An external, encryption-related error occurred	Check the encryption setting on your device class and tape drive.
426	X'1AB'	A CRC mismatch occurred	Ensure that the media has not reached the end of life as specified by the media manufacturer. Try the operation again.

Descriptions of standard ASC and ASCQ codes

Standard ASC and ASCQ codes are described.

The ASC and ASCQ codes are bytes 12 and 13 for SCSI-2 devices. On Windows systems, these codes are displayed in the Windows Event Log, but the information is in different bytes.

See server message ANR8300E or ANR8302E for the recommended action.

The following table provides standard descriptions for some ASC and ASCQ codes. Each value has a prefix of 0x, which indicates that it is a hexadecimal constant. Note that descriptions vary among devices. For an accurate description of ASC and ASCQ codes for any device, see the documentation that comes with the device.

Table 1. Descriptions of standard ASC and ASCQ codes

ASC	ASCQ	Description
0x00	0x00	No additional sense
0x00	0x01	Filemark detected
0x00	0x02	End-of-medium detected
0x00	0x03	Setmark detected
0x00	0x04	Beginning of medium
0x00	0x05	End of data
0x00	0x06	I/O process terminated
0x02	0x00	No seek complete
0x03	0x00	Device write fault
0x03	0x01	No write current
0x03	0x02	Excessive write errors
0x04	0x00	Logical unit not ready
0x04	0x01	Becoming ready
0x04	0x02	Not ready, initializing command required

ASC	ASCQ	Description
0x04	0x03	Not ready, manual intervention required
0x04	0x04	Not ready, formatting
0x05	0x00	No response to select
0x06	0x00	No reference position found
0x07	0x00	Multiple devices selected
0x08	0x00	Communication failure
0x08	0x01	Communication timeout
0x08	0x02	Communication parity error
0x09	0x00	Track following error
0x0A	0x00	Error log overflow
0x0C	0x00	Write error
0x11	0x00	Unrecovered read error
0x11	0x01	Read retries exhausted
0x11	0x02	Error too long to correct
0x11	0x03	Multiple read errors
0x11	0x08	Incomplete block read
0x11	0x09	No gap found
0x11	0x0A	Miscorrected error
0x14	0x00	Recorded entity not found
0x14	0x01	Record not found
0x14	0x02	Filemark/setmark not found
0x14	0x03	End-of-data not found
0x14	0x04	Block sequence error
0x15	0x00	Random positioning error
0x15	0x01	Mechanical positioning error
0x15	0x02	Read positioning error
0x17	0x00	No error correction applied
0x17	0x01	Recovered with retries
0x17	0x02	Recovered with positive head offset
0x17	0x03	Recovered with negative head offset
0x18	0x00	ECC applied
0x1A	0x00	Parameter list length error
0x1B	0x00	Synchronous data transfer error
0x20	0x00	Invalid operation code
0x21	0x00	Block out of range
0x21	0x01	Invalid element address
0x24	0x00	Invalid field in CDB
0x25	0x00	LUN not supported
0x26	00	Invalid field in parameter list
0x26	0x01	Parameter not supported

ASC	ASCQ	Description
0x26	0x02	Parameter value invalid
0x26	0x03	Threshold parameters not supported
0x27	0x00	Write protected
0x28	0x00	Not-ready to ready
0x28	0x01	Import/export element accessed
0x29	0x00	Power-on, reset, bus reset
0x2A	0x00	Parameters changed
0x2A	0x01	Mode parameters changed
0x2A	0x02	Log parameters changed
0x2B	0x00	Copy cannot run
0x2C	0x00	Command sequence error
0x2D	0x00	Overwrite error on update
0x2F	0x00	Command cleared by initiator
0x30	0x00	Incompatible media
0x30	0x01	Media unknown format
0x30	0x02	Media incompatible format
0x30	0x03	Cleaning cartridge installed
0x31	0x00	Media format corrupted
0x33	0x00	Tape length error
0x37	0x00	Rounded parameter
0x39	0x00	Saving parameters not supported
0x3A	0x00	Medium not present
0x3B	0x00	Sequential positioning error
0x3B	0x01	Positioning error at BOT
0x3B	0x02	Positioning error at EOT
0x3B	0x08	Reposition error
0x3B	0x0D	Medium destination element full
0x3B	0x0E	Medium source element empty
0x3D	0x00	Invalid bits in message
0x3E	0x00	LUN not self-configured
0x3F	0x00	Operating conditions changed
0x3F	0x01	Microcode changed
0x3F	0x02	Changed operating definition
0x3F	0x03	Inquiry data changed
0x3F	0x0E	Reported LUNs data changed
0x43	0x00	Message error
0x44	0x00	Internal target failure
0x45	0x00	Select/reselect failure
0x46	0x00	Unsuccessful soft reset
0x47	0x00	SCSI parity error

ASC	ASCQ	Description
0x48	0x00	Initiator detected message received
0x49	0x00	Invalid message error
0x4A	0x00	Command phase error
0x4B	0x00	Data phase error
0x4C	0x00	LUN failed self-configuration
0x4E	0x00	Overlapped commands attempt
0x50	0x00	Write append error
0x50	0x01	Write append position error
0x50	0x02	Position error (timing)
0x51	0x00	Erase failure
0x52	0x00	Cartridge fault
0x53	0x00	Load/media eject failed
0x53	0x01	Unload tape failure
0x53	0x02	Media removal prevented
0x5A	0x00	Operator state changed
0x5A	0x01	Operator media removal
0x5A	0x02	Operator write protect
0x5A	0x03	Operator write permit
0x5B	0x00	Log exception
0x5B	0x01	Threshold condition met
0x5B	0x02	Log counter at maximum
0x5B	0x03	Log list codes exhausted

- ASC and ASCQ codes in the Windows Event Log
  ASC and ASCQ codes are displayed in the Windows Event Log.

Device error codes in the AIX system error log

Some device error codes are logged in the AIX® system error log.

ADSM_DD_LOG1 (0xAC3AB953)
DEVICE DRIVER SOFTWARE ERROR

This error is logged by the IBM Spectrum Protect™ device driver when a problem is suspected in the IBM Spectrum Protect device driver software. If the IBM Spectrum Protect device driver issues a SCSI I/O command with an illegal operation code, the command fails and the error is logged with this identifier. Report this error immediately to IBM Spectrum Protect Support.

Detail Data: Sense Data

The sense data contains information that can determine the cause of the error. Report all data in the error entry to IBM Spectrum Protect Support.

ADSM_DD_LOG2 (0x5680E405)
HARDWARE/COMMAND-ABORTED ERROR

This error is logged by the IBM Spectrum Protect device driver when the device reports a hardware error or stop-command error in response to a SCSI I/O command.

Detail Data: Sense Data

The sense data contains information that can determine which hardware component failed and why. To interpret the sense data for a particular device, refer to the SCSI specification manual for the device.

ADSM_DD_LOG3 (0x461B41DE)
MEDIA ERROR

This error is logged by the IBM Spectrum Protect device driver when a SCSI I/O command fails because of corrupted or incompatible media, or because a drive requires cleaning.

Detail Data: Sense Data

The sense data contains information that can determine the cause of the error. To interpret the sense data for a particular device, refer to the SCSI specification manual for the device.

ADSM_DD_LOG4 (0x4225DB66)
TARGET DEVICE GOT UNIT ATTENTION

This error is logged by the IBM Spectrum Protect device driver after receiving certain UNIT ATTENTION notifications from a device. UNIT ATTENTIONs are informational and usually indicate that some state of the device changed. For example, this error would be logged if the door of a library device was opened and then closed. Logging this event indicates that the activity occurred and that the library inventory might be changed.

Detail Data: Sense Data

The sense data contains information that describes the reason for the UNIT ATTENTION. To interpret the sense data for a particular device, see the SCSI specification manual for the device.

ADSM_DD_LOG5 (0xDAC55CE5)
PERMANENT UNKNOWN ERROR

This error is logged by the IBM Spectrum Protect device driver after receiving an unknown error from a device in response to a SCSI I/O command. If the error persists, report it to IBM Spectrum Protect support personnel.

Detail Data: Sense Data

The sense data consists of information that can determine the cause of the error. Report all data in the error entry to IBM Spectrum Protect Support.

ADSM_DD_LOG6 (0xBC539B26)
WARNING OR INFORMATIONAL MESSAGE FOR TARGET DEVICE

This error is logged by the IBM Spectrum Protect device driver after receiving a warning or informational message from a device in response to a SCSI I/O command. These warning or informational messages might not be an indication of a problem. They could be an indication that cleaning is completed, that the cleaning cartridge is inserted, or something similar. If the message persists, report it to IBM Spectrum Protect Support.

Detail Data: Sense Data

The sense data consists of information that can determine the reason for the message. Report all data in the entry to IBM Spectrum Protect Support.

IBM Global Security Kit return codes

The server and client use the IBM Global Security Kit (GSKit) for SSL (Secure Sockets Layer) processing between the server and the backup-archive client. Some messages that are issued for SSL processing include GSKit return codes.

GSKit is automatically installed or updated during IBM Spectrum Protect™ installation and provides the following libraries:

- GSKit SSL
- GSKit Key Management API
- IBM Crypto for C (ICC)

The tsmdiag utility reports the GSKit level that is installed on your system, or you can use one of the following methods:

- For Windows, issue the following commands:

```
regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"
notepad gskitinfo.txt
```

CAUTION:
You can damage the system registry if you use regedit incorrectly.

- For the 64-bit AIX® server, issue the following command from the command line: `gsk8ver_64`

See Table 1 for the GSKit SSL return codes.

The server uses the GSKit Key Management API to automatically create the key management database and server private and public keys. Some messages that are issued for this processing might include GSKit Key Management return codes. See Table 2 for the key management return codes.

Table 1. IBM Global Security Kit SSL general return codes

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000000	0	GSK_OK	The task completes successfully. Issued by every function call that completes successfully.
0x00000001	1	GSK_INVALID_HANDLE	The environment or SSL handle is not valid. The specified handle was not the result of a successful `open()` function call.
0x00000002	2	GSK_API_NOT_AVAILABLE	The dynamic link library (DLL) was unloaded and is not available (occurs on Microsoft Windows systems only).
0x00000003	3	GSK_INTERNAL_ERROR	Internal error. Report this error to IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Insufficient memory is available to complete the operation.
0x00000005	5	GSK_INVALID_STATE	The handle is not in a valid state for operation, such as completing an `init()` operation on a handle twice.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Specified key label is not found in key file.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Certificate is not received from the partner.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Certificate validation error.
0x00000009	9	GSK_ERROR_CRYPTO	Error processing cryptography.
0x0000000a	10	GSK_ERROR_ASN	Error validating ASN fields in certificate.
0x0000000b	11	GSK_ERROR_LDAP	Error connecting to user registry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Internal error. Report this error to IBM Software Support.
0x0000000d	13	GSK_INVALID_PARAMETER	Invalid parameter.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Invalid parameter. Report this error to IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Internal error. Report this error to IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	I/O error reading the key file.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	The key file does not have a valid internal format. Recreate the key file.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	The key file has two entries with the same key.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	The key file has two entries with the same label.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	The key file password is used as an integrity check. Either the key file is corrupted or the password ID is incorrect.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	The default key in the key file has an expired certificate.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	An error occurred loading one of the GSK dynamic link libraries. Check that GSK was installed correctly.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indicates that a connection is trying to be made in a GSK environment after the GSK_ENVIRONMENT_ CLOSE_OPTIONS was set to GSK_DELAYED_ ENVIRONMENT_CLOSE and gsk_environment_close() function was called.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Both the password and the stash-file name were not specified. The key file is not initialized.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Unable to open the key file. Either the path was specified incorrectly or the file permissions did not allow the file to be opened.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Unable to generate a temporary key pair. Report this error to IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	A user name object was specified that is not found.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	A password that is used for an LDAP (lightweight directory access protocol) query is not correct.
0x000000ce	206	GSK_ERROR_BAD_INDEX	An index into the Fail Over list of LDAP servers was not correct.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	This installation of GSKit does not support FIPS mode of operation.
0x0000012d	301	GSK_CLOSE_FAILED	Indicates that the GSK environment close request was not properly managed. Cause is most likely due to a gsk_secure_socket*() command that is attempted after a gsk_close_environment() call.
0x00000191	401	GSK_ERROR_BAD_DATE	The system date was not set to a valid value.
0x00000192	402	GSK_ERROR_NO_CIPHERS	The SSLv2 and the SSLv3 are not enabled.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	The required certificate was not received from the partner.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	The received certificate was formatted incorrectly.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	The received certificate type was not supported.
0x00000196	406	GSK_ERROR_IO	An I/O error occurred on a data read or write operation.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	The specified label in the key file is not found.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	The specified key file password is incorrect. The key file cannot be used. The key file also might be corrupt.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	In a restricted cryptography environment, the key size is too long to be supported.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	An incorrectly formatted SSL message was received from the partner.
0x0000019b	411	GSK_ERROR_BAD_MAC	The message authentication code (MAC) was not successfully verified.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Unsupported SSL protocol or unsupported certificate type.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	The received certificate contained an incorrect signature.
0x0000019e	414	GSK_ERROR_BAD_CERT	Incorrectly formatted certificate is received from the partner.
0x0000019f	415	GSK_ERROR_BAD_PEER	Did not receive a valid SSL protocol from the partner.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Report this error to IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	The self-signed certificate is not valid.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	The `read()` failed. Report this error to IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	The `write()` failed. Report this error to IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	The partner closed the socket before the protocol completed.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	The specified V2 cipher is not valid.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	The specified V3 cipher is not valid.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Report this error to IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Report this error to IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	The handle cannot be created. Report this error to IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialization failed. Report this internal error to service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Not able to access the specified user registry when a certificate is being validated.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	The specified key did not contain a private key.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	A failed attempt was made to load the specified PKCS11 shared library.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	The PKCS #11 driver failed to find the token that is specified by the caller.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	A PKCS #11 token is not present in the slot.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	The password/pin to access the PKCS #11 token is not valid.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	The SSL header received was not a properly formatted SSLv2 header.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000001b2	434	GSK_CSP_OPEN_ERROR	Cannot open the hardware-based cryptographic service provider. Either the CSP name is not specified correctly or a failed attempt was made to access the specified CSP certificate store.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Attribute setting conflict between PKCS11, CMS key database, and Microsoft Crypto API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	The requested function is not supported on the platform that the application is running. For example, the Microsoft Crypto API is not supported on platforms other than Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Incorrect value is returned from the reset session type callback function. Only GSKit `gsk_sever_session`, `gsk_sever_session_with_cl_auth`, or `gsk_sever_session_with_cl_auth_crit` is allowed.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	The buffer size is negative or zero.
0x000001f6	502	GSK_WOULD_BLOCK	Used with nonblocking I/O. Refer to the nonblocking section for usage.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 is required for `reset_cipher()`, and the connection uses SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	A valid ID was not specified for the `gsk_secure_soc_misc()` function call.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	The function call does not have a valid ID. This issue might also be caused by specifying an environment handle when a handle for an SSL connection should be used.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	The attribute has a negative length, which is not valid.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	The enumeration value is not valid for the specified enumeration type.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	A parameter list that is not valid for replacing the SID cache routines.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	When a numeric attribute is set, the specified value is not valid for the specific attribute that is being set.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Conflicting parameters were set for additional certificate validation.
0x000002c3	707	GSK_AES_UNSUPPORTED	The AES cryptographic algorithm is not supported.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	The PEERID does not have the correct length.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OF F	The particular cipher is not allowed when FIPS mode of operation is off.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No approved FIPS ciphers are selected in FIPS mode of operation.
0x00000641	1601	GSK_TRACE_STARTED	The trace started successfully.
0x00000642	1602	GSK_TRACE_STOPPED	The trace stopped successfully.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000643	1603	GSK_TRACE_NOT_STARTED	No trace file was previously started, so it cannot be stopped.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Trace file is started, so it cannot be restarted.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Trace file cannot be opened. The first parameter of `gsk_start_trace()` must be a valid full path file name.

Table 2. IBM Global Security Kit key management return codes

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000000	0	GSK_OK	The task completes successfully. This message is issued by every function call that completes successfully.
0x00000001	1	GSK_INVALID_HANDLE	The environment or SSL handle is not valid. The specified handle was not the result of a successful open() function call.
0x00000002	2	GSK_API_NOT_AVAILABLE	The DLL (dynamic link library) was unloaded and is not available (occurs on Microsoft Windows systems only).
0x00000003	3	GSK_INTERNAL_ERROR	Internal error. Report this error to IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Insufficient memory is available to complete the operation.
0x00000005	5	GSK_INVALID_STATE	The handle is in an incorrect state for operation, such as completing an init() operation on a handle twice.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Specified key label is not found in key file.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Certificate is not received from the partner.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Certificate validation error.
0x00000009	9	GSK_ERROR_CRYPTO	Error processing cryptography.
0x0000000a	10	GSK_ERROR_ASN	Error validating ASN fields in certificate.
0x0000000b	11	GSK_ERROR_LDAP	Error connecting to user registry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Internal error. Report this error to IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Internal error. Report this error to IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	I/O error reading the key file.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	The key file has an internal format that is not valid. Recreate key file.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	The key file has two entries with the same key.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	The key file has two entries with the same label.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_ PASSWORD	The key file password is used as an integrity check. Either the key file is corrupted or the password ID is incorrect.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	The default key in the key file has an expired certificate.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	An error occurred while one of the GSK dynamic link libraries is loaded. Check GSK was installed correctly.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	This message indicates that a connection is trying to be made in a GSK environment after the GSK_ENVIRONMENT_ CLOSE_OPTIONS was set to GSK_DELAYED_ ENVIRONMENT_CLOSE and gsk_environment_close() function was called.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Both the password and the stash-file name were not specified, so the key file is not initialized.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Unable to open the key file. Either the path was specified incorrectly or the file permissions did not allow the file to be opened.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Unable to generate a temporary key pair. Report this error to IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	A user name object was specified that is not found.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_ CREDENTIALS	A Password that is used for an LDAP query is not correct.
0x000000ce	206	GSK_ERROR_BAD_INDEX	An index into the Fail Over list of LDAP servers was not correct.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	This installation of GSKit does not support FIPS mode of operation.
0x0000012d	301	GSK_CLOSE_FAILED	Indicates that the GSK environment close request was not properly managed. Cause is most likely due to attempting a gsk_secure_socket*() command after a gsk_close_environment() call.
0x00000191	401	GSK_ERROR_BAD_DATE	The system date was set to a value that is not valid.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 and SSLv3 are not enabled.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	The required certificate was not received from the partner.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	The received certificate was formatted incorrectly.
0x00000195	405	GSK_ERROR_UNSUPPORTED_ CERTIFICATE_TYPE	The received certificate type was not supported.
0x00000196	406	GSK_ERROR_IO	An I/O error occurred on a data read-or-write operation.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	The specified label in the key file is not found.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	The specified key file password is incorrect. The key file cannot be used. The key file might also be corrupt.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_ FOR_EXPORT	In a restricted cryptography environment, the key size is too long to be supported.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	An incorrectly formatted SSL message was received from the partner.
0x0000019b	411	GSK_ERROR_BAD_MAC	The MAC was not successfully verified.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Unsupported SSL protocol or unsupported certificate type.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	The received certificate contained an incorrect signature.
0x0000019e	414	GSK_ERROR_BAD_CERT	Incorrectly formatted certificate is received from the partner.
0x0000019f	415	GSK_ERROR_BAD_PEER	An SSL protocol that is not valid is received from the partner.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Report this error to IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	The self-signed certificate is not valid.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	The read() failed. Report this error to IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	The write() failed. Report this error to IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	The partner closed the socket before the protocol completed.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	The specified V2 cipher is not valid.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	The specified V3 cipher is not valid.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Report this error to IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_ COMBINATION	Report this error to IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_ FAILED	The handle is not created. Report this error to IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialization failed. Report this internal error to service.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Unable to access the specified user registry when a certificate is being validated
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	The specified key did not contain a private key.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_ NOTLOADED	A failed attempt was made to load the specified PKCS11 shared library.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_ LABELMISMATH	The PKCS #11 driver failed to find the token that is specified by the caller.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_ NOTPRESENT	A PKCS #11 token is not present in the slot.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_ BADPASSWORD	The password/pin to access the PKCS #11 token is incorrect.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	The SSL header received was not a properly formatted SSLv2 header.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Could not open the hardware-based cryptographic service provider (CSP). Either the CSP name is not specified correctly or a failed attempt was made to access the specified CSP certificate store.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Some conflicting attributes for SSL operation were defined.
0x000001b4	436	GSK_CSP_OPEN_ERROR	The Microsoft Crypto API is only supported on Microsoft Windows 2000 with Service Pack 2 applied.
0x000001b5	437	GSK_CSP_OPEN_ERROR	System is running in IPv6 mode without setting a PEERID.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	The buffer size is negative or zero.
0x000001f6	502	GSK_WOULD_BLOCK	Used with nonblocking I/O. Refer to the nonblocking section for usage.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 is required for reset_cipher(), and the connection uses SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	An ID that is not valid was specified for the gsk_secure_soc_misc() function call.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	The function call has an ID that is not valid. This issue might also be caused by specifying an environment handle when a handle for an SSL connection should be used.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	The attribute has a negative length, which is not valid.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ ENUMERATION	The enumeration value is not valid for the specified enumeration type.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	A parameter list that is not valid for replacing the SID cache routines.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_ NUMERIC_VALUE	When a numeric attribute is set, the specified value is not valid for the specific attribute that is being set.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_ SETTING	Conflicting parameters were set for additional certificate validation.
0x000002c3	707	GSK_AES_UNSUPPORTED	The AES cryptographic algorithm is not supported.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	The PEERID does not have the correct length.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	The particular cipher is not allowed when FIPS mode of operation is off.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No approved FIPS ciphers are selected in FIPS mode of operation.
0x00000641	1601	GSK_TRACE_STARTED	The trace started successfully.
0x00000642	1602	GSK_TRACE_STOPPED	The trace stopped successfully.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No trace file was previously started so it cannot be stopped.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Trace file is started so it cannot be started again.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Trace file cannot be opened. The first parameter of gsk_start_trace() must be a valid, full-path file name.

Глоссарий

В этом глоссарии собраны термины и определения для IBM Spectrum Protect и связанных продуктов.

В этом глоссарии используются следующие виды перекрестных ссылок:

- *Смотрите* указывает на более предпочтительный термин по сравнению с менее предпочтительным или на полную форму термина по сравнению с сокращением.
- *Смотрите также* указывает на родственный термин или термин с противоположным значением.

Информацию о других терминах и определениях смотрите на веб-сайте IBM Terminology.

A C D E F G H I L M N S T U V W А Б В Г Д Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Э

A

ACK
: Смотрите подтверждение.

ACL
: Смотрите список управления доступом.

AutoFS
: Смотрите автоматически монтируемая файловая система.

C

CAD
: Смотрите client acceptor daemon.

client acceptor daemon (CAD)
: Смотрите client acceptor.

D

DRM
: Смотрите менеджер аварийного восстановления.

DSMAPI
: Смотрите интерфейс прикладного программирования управления хранением данных.

E

EA
: Смотрите расширенный атрибут.

EFS
: Смотрите Encrypted File System.

Encrypted File System (EFS)
: Файловая система, в которой используется шифрование на уровне файловой системы.

F

File System Migrator (FSM)
: Расширение ядра, которое перехватывает все операции файловой системы и обеспечивает всю необходимую поддержку управления пространством. Если поддержка управления пространством не нужна, операция передается операционной системе, которая будет выполнять свои обычные функции. При добавлении управление пространством в файловую системы поверх файловой системы монтируется функция переноса данных для файловой системы (File System Migrator - FSM).

FSID
: Смотрите ID файлового пространства.

FSM
: Смотрите file system migrator.

G

General Parallel File System (GPFS)
: Высокопроизводительная файловая система на совместно используемом диске, способная обеспечить доступ к данным в кластеризованной системной среде. Смотрите также управление жизненным циклом информации.

GPFS
: Смотрите General Parallel File System.

GUID
: Смотрите глобальный уникальный идентификатор.

H

HSM
: Смотрите управление иерархическим пространством.

I

ILM
: Смотрите управление жизненным циклом информации.

inode
: Внутренняя структура, описывающая отдельные файлы в системах AIX, UNIX или Linux. Inode содержит информацию об узле, типе, владельце и положении файла.

IP-адрес (IP address)
: Уникальный адрес устройства или логического устройства в сети, в которой используется стандарт Internet Protocol (IP).

L

LAN

Смотрите локальная сеть.

LOFS
: Смотрите loopback virtual file system.

Logical Volume Snapshot Agent (LVSA)
: Программа, которая может функционировать в качестве провайдера снимков, создавая снимок логического тома в ходе онлайнового резервного копирования образа..

Loopback Virtual File System (LOFS)
: Файловая система, которая создается путем монтирования каталога поверх другого локального каталога; также называется монтированием поверх монтирования. LOFS также может создаваться средством автоматического монтирования.

LUN
: Смотрите номер логического устройства.

LVSA
: Смотрите Logical Volume Snapshot Agent.

M

MTU
: Смотрите максимальный размер блока передачи.

N

NDMP
: Смотрите Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)
: Стандартный интерфейс сетей и персональных компьютеров, используемый в локальных сетях для обеспечения функций передачи сообщений, сервера печати и файл-сервера. Прикладным программам, использующим NetBIOS, не нужно обрабатывать детали протоколов DLC (Data Link Control) для локальной сети.

Network Basic Input/Output System
: Смотрите NetBIOS.

Network Data Management Protocol (NDMP)
: Протокол, который позволяет сетевым программам, осуществляющим управление хранением, управлять операциями резервного копирования и восстановления на NDMP-совместимом файл-сервере, не устанавливая на нем никаких приобретенных у поставщиков программ.

S

SAN
: Смотрите storage area network.

Secure Sockets Layer (SSL)
: Протокол защиты, обеспечивающий конфиденциальность связи. При помощи SSL программы структуры "клиент-сервер" могут связываться друг с другом с исключением возможностей подслушивания, подделки и искажения сообщений.

SSL
: Смотрите Secure Sockets Layer.

T

TCA
: Смотрите trusted communications agent.

TCP/IP
: Смотрите TCP/IP (Transmission Control Protocol/Internet Protocol).

Transmission Control Protocol/Internet Protocol (TCP/IP)
: Непатентованный набор протоколов связи промышленного стандарта, который обеспечивает надежное соединение между программами на двух конечных точках по сопряженным сетям разных типов. Смотрите также способ связи.

U

UCS-2

2-байтная (16-битная) схема кодировки на основе спецификации ISO/IEC 10646-1. UCS-2 определяет три уровня реализации: Уровень 1 - не разрешены никакие сочетания элементов кодировок; Уровень 2 - разрешены сочетания элементов кодировок только для тайского, индийского, иврита и арабского; Уровень 3 - разрешены любые сочетания элементов кодировок.

UNC
: Смотрите Universal Naming Convention.

Unicode
: Стандарт кодировки символов, который поддерживает обмен текстовыми данными, обработку и вывод текста, записанного на общепринятых языках на земном шаре, плюс многих классических и исторических текстов.

Universally Unique Identifier (UUID)
: 128-битный числовой идентификатор, позволяющий гарантировать, что у двух компонентов не будет одного и того же идентификатора. Смотрите также глобальный уникальный идентификатор.

Universal Naming Convention (UNC)
: Комбинация имени сервера и имени сети. Эти имена вместе указывают ресурс в домене.

UTF-8
: Формат Unicode Transformation Format, 8-разрядная форма кодировки, предназначенная для использования вместе с существующими системами на основе ASCII. Значение CCSID для данных в формате UTF-8 - 1208.

UUID
: Смотрите Universally Unique Identifier.

V

Volume Shadow Copy Service (VSS)
: Набор интерфейсов прикладного программирования (application-programming interface, API) Microsoft, используемых для создания теневых копий томов и точных копий файлов, включая все открытые файлы, и т.д.

VSS
: Смотрите Volume Shadow Copy Service.

W

WPAR
: Смотрите раздел рабочей нагрузки.

WWN
: Смотрите глобальное имя.

A

абсолютный режим (absolute mode)
: В управлении хранением данных: Режим группы резервных копий, при котором файл или каталог подлежит инкрементному резервному копированию, даже если файл или каталог не изменился со времени создания его последней резервной копии. Смотрите также режим, измененный режим.

автоматический перенос (automatic migration)
: Процедура, используемая для автоматического переноса файлов из локальной файловой системы в хранилище с учетом опций и параметров, выбранных пользователем root на рабочей станции. Смотрите также перенос по запросу, пороговый перенос.

автоматически монтируемая файловая система (automounted file system, AutoFS)
: Файловая система, управляемая демоном automounter. Демон automounter осуществляет мониторинг указанного пути каталога и автоматически монтирует файловую системы для обеспечения доступа к данным.

автоматическое определение (automatic detection)
: Функция, которая обнаруживает, сообщает и обновляет серийный номер устройства или библиотеки в базе данных при создании определения пути с локального сервера.

автономное резервное копирование тома (offline volume backup)
: Резервное копирование, при котором том блокируется, так чтобы никакие другие системные программы не могли обращаться к нему во время выполнения операции резервного копирования.

авторизованный пользователь (authorized user)
: Пользователь, у которого есть административные права доступа к клиенту на рабочей станции. Этот пользователь может изменять пароли, производить открытую регистрацию и удалять файловые пространства.

агент TCA (trusted communications agent, TCA)
: Программа, которая обрабатывает протокол с использованием пароля для входа в систему, когда клиенты применяют генерирование пароля.

агент хранения (storage agent)

Программа, которая позволяет производить резервное копирование данных клиента непосредственно в хранилище, соединенное с сетью хранения данных (Storage Area Network - SAN), и восстановление данных клиента непосредственно из этого хранилища.

агрегат (aggregate)
Объект, представляющий собой группу логических файлов, резервное копирование или архивирование которых выполняется за одну транзакцию; агрегат содержится в пулах хранения в виде одного физического файла. Смотрите также логический файл, физический файл.

адаптивное субфайловое резервное копирование (adaptive subfile backup)
Тип резервного копирования, при котором на сервер отправляются только изменившиеся части файла, а не весь файл. Адаптивное субфайловое резервное копирование позволяет снизить сетевой трафик и повысить скорость резервного копирования.

администратор (administrator)
Лицо, отвечающее за такие административные задачи, как авторизация доступа и управление содержимым. Администраторы также могут предоставлять пользователям полномочия того или иного уровня.

активировать (activate)
Проверить содержимое набора политик и сделать его активным набором политик.

активная версия (active version)
Самая последняя сохраненная резервная копия файла. Активную версию файла нельзя удалить, пока процедура резервного копирования не установит, что пользователь заменил этот файл на более новую версию либо удалил файл с рабочей станции или файл-сервера. Смотрите также версия резервной копии, неактивная версия.

активная файловая система (active file system)
Файловая система, в которую было добавлено управление пространством. При использовании управления пространством задачи для активной файловой системы включают в себя автоматический перенос, согласование, выборочный перенос и возврат. Смотрите также неактивная файловая система.

активный набор политики (active policy set)
Активированный набор правил политики, который содержит правила политики, используемые в настоящий момент всеми клиентскими узлами, относящимися к данному домену политики. Смотрите также домен политики, набор правил политики.

алгоритм Нейгла (Nagle algorithm)
Алгоритм, который позволяет снизить загрузку сетей TCP/IP путем объединения мелких пакетов и их совместной отправки.

архивирование (archive)
Копирование программ, данных или файлов на другой носитель, обычно для долгосрочного хранения или с целью обеспечения защиты. Смотрите также получить.

архивная копия (archive copy)
Файл или группа файлов, помещенные в архив в системе хранения сервера.

аудит (audit)
Проверка наличия логических несоответствий между сведениями на сервере и фактическим состоянием системы. Менеджер хранения может производить аудит информации о таких элементах, как тома, библиотеки и лицензии. Например, когда менеджер хранения производит аудит тома, сервер проверяет наличие противоречий между информацией о резервных копиях файлов или заархивированных файлах, хранящихся в базе данных, и фактическими данными, связанными с каждой резервной версией или архивной копией в серверном хранилище.

Б

база данных предварительно перенесенных файлов (premigrated files database)
База данных, содержащая информацию о каждом файле, который был предварительно перенесен в серверное хранилище.

библиотека (library)

1. Репозиторий съемных носителей, например магнитных дисков и магнитных лент.
2. Собрание из одного или нескольких накопителей и, возможно, робототехнических устройств (это зависит от типа библиотеки), которые могут использоваться для доступа к томам хранения.

быстрое восстановление VSS (VSS Fast Restore)
Операция, которая восстанавливает данные из локального снимка. Снимок - это резервная копия VSS, которая находится на локальном теневом томе. Операция восстановления получает данные, используя метод копирования на уровне файлов.

В

версия (version)

Резервная копия файла в серверном хранилище. Последняя резервная копия файла является активной версией. Более ранние копии этого же файла - неактивные версии. Число версий, сохраняемых сервером, определяется атрибутами группы копий в классе управления.

взаимосвязь (association)
Заданное взаимоотношение между клиентским узлом и запланированным заданием клиента. Связь определяет имя расписания, имя домена политики, которому оно принадлежит, и имя клиентского узла, выполняющего назначенные операции.

виртуальная точка монтирования (virtual mount point)
Ветвь каталога файловой системы, заданная как виртуальная файловая система. Резервная копия виртуальной файловой системы создается в ее собственном файловом пространстве на сервере. Сервер обрабатывает виртуальную точку монтирования как отдельную файловую систему, но операционная система клиента этого не делает.

виртуальное файловое пространство (virtual file space)
Способ представления каталога в файловой системе NAS (Network-Attached Storage) в виде пути к этому каталогу.

виртуальный том (virtual volume)
Архивный файл на сервере назначения, представленный для исходного сервера как том с последовательным доступом.

внешний формат данных (non-native data format)
Формат записи данных в пул хранения, отличный от формата, используемого сервером при выполнении операций. Смотрите также внутренний формат данных.

внешняя библиотека (external library)
Собрание накопителей, управляемое системой управления носителями, отличающейся от сервера управления хранением.

внутренний формат данных (native format)
Формат данных, непосредственно записываемых в пул хранения сервером. Смотрите также внешний формат данных.

возврат (recall)
Копирование перенесенного файла из серверного хранилища обратно в исходную файловую систему с использованием клиента управления иерархическим хранением. Смотрите также выборочный возврат.

возраст файла (file age)
В применении к приоритету файлов для переноса: число дней с момента последнего обращения к файлу.

восстановление (restore)
Копирование данных из положения их резервной копии в активное положение хранения для дальнейшего использования. Например, копирование информации из системы хранения сервера на рабочую станцию-клиент.

восстановление VSS (VSS Restore)
Функция, которая использует аппаратный провайдер Microsoft Volume Shadow Copy Service (VSS) для восстановления снимков, находящихся в серверном хранилище. Снимки были созданы операцией резервного копирования VSS и восстановлены в их исходное расположение.

восстановление индивидуального почтового ящика (individual mailbox restore)
Смотрите восстановление почтового ящика.

восстановление почтового ящика (mailbox restore)
Функция, обеспечивающая восстановление данных Microsoft Exchange Server (из резервных копий IBM Data Protection for Microsoft Exchange) на уровне почтового ящика или на уровне элементов почтового ящика.

время доступа к файлу (file access time)
В системах AIX, UNIX и Linux: время последнего обращения к файлу.

встроенная дедупликация данных (inline data deduplication)
Способ сокращения объема пространства, необходимого для хранения данных, исключением излишних данных. При записи в пул хранения контейнеров данные дедуплицируются. Смотрите также дедупликация данных, дедупликация данных после обработки.

встроенное сжатие (inline compression)
Метод сокращения пространства хранения. Повторяющиеся символы, пробелы, строки символов или двоичные данные удаляются при записи данных в пул хранения контейнеров. Смотрите также сжатие.

вторичный узел (secondary site)
Физический или виртуальный узел, состоящий из аппаратных и сетевых ресурсов и ресурсов хранения, которые поддерживают восстановление первичного узла. При отказе первичного узла выполнение операций может продолжаться на вторичном узле. Смотрите также первичный узел.

выборочное резервное копирование (selective backup)
Процесс резервного копирования отдельных файлов или каталогов из домена клиента. Производится резервное копирование файлов, которые не являются исключенными в списке включения-исключения. Эти файлы должны соответствовать требованиям к сериализации, заданным в группе резервных копий класса управления, назначенного для каждого файла. Смотрите также инкрементное резервное копирование.

выборочный возврат (selective recall)

Процесс копирования выбранных пользователем файлов из серверного хранилища в локальную файловую систему. Смотрите также возврат, прозрачный возврат.

выборочный перенос (selective migration)
Процесс копирования выбранных пользователем файлов из локальной файловой системы в серверное хранилище и их замены в локальной файловой системе на стаб-файлы. Смотрите также перенос по запросу, пороговый перенос.

высвобождение (reclamation)
Процесс сбора данных, оставшихся на нескольких томах с последовательным доступом, на меньшем числе других томов с последовательным доступом.

Г

ГБ (GB)
Смотрите гигабайт.

генерирование пароля (password generation)
Процесс, который создает и сохраняет новый пароль в зашифрованном файле пароля, когда истекает срок действия прежнего пароля. При автоматическом генерировании пароля запрос о пароле не появляется.

гигабайт, ГБ (gigabyte, GB)
В применении к процессорной памяти, реальной и виртуальной памяти и объему канала: два в 30-й степени или 1 073 741 824 байт. В применении к дисковой памяти и объему информации при осуществлении взаимодействий: 1 000 000 000 байт.

глобальное имя (worldwide name, WWN)
64-битный (без знака) уникальный идентификатор имени.

глобально неактивное состояние (global inactive state)
Состояние всех файловых систем, в которые было добавлено управление пространством, после глобальной деактивации управления пространством для клиентского узла.

глобальный уникальный идентификатор (globally unique identifier - GUID)
Задаваемое в соответствии с алгоритмом число, позволяющее однозначно идентифицировать объект в системе. Смотрите также Universally Unique Identifier.

группа архивных копий (archive copy group)
Объект политики, который содержит атрибуты, управляющие генерированием, местом назначения и сроком действия заархивированных файлов. Смотрите также группа копий.

группа копий (copy group)
Объект политики, содержащий атрибуты, которые определяют порядок создания, пул назначения и условия устаревания архивных и резервных копий файлов. Группа копий относится к классу управления. Смотрите также группа архивных копий, группа резервных копий, версия резервной копии, класс управления.

группа резервных копий (backup copy group)
Объект политики, который содержит атрибуты, управляющие генерированием, пунктом назначения и устареванием версий резервных копий файлов. Группа резервных копий относится к классу управления. Смотрите также группа копий.

группа совместного размещения (collocation group)
Заданная пользователем группа клиентских узлов, чьи данные в процессе совместного размещения сохраняются на минимальном числе томов.

Д

дедупликация данных (data deduplication)
Способ сокращения объема пространства, необходимого для хранения данных, исключением излишних данных. На носителе сохраняется только один экземпляр данных. Другие экземпляры тех же данных заменяются указателем на сохраненный экземпляр. Смотрите также встроенная дедупликация данных, дедупликация данных после обработки.

дедупликация данных после обработки (postprocess data deduplication)
Способ сокращения объема пространства, необходимого для хранения данных, исключением излишних данных. Сначала данные записываются в пул хранения, после чего выявляются дубликаты данных, а затем высвобождается пространство в пуле хранения. Смотрите также дедупликация данных, встроенная дедупликация данных.

демон (daemon)
Программа, которая работает без участия пользователя, постоянно или периодически выполняя такие функции, как управление сетью.

демон журнала (journal daemon)
В системах AIX, UNIX и Linux: Программа, которая следит за активностью файлов, находящихся в файловых системах.

демон монитора пространства (space monitor daemon)

Демон, который проверяет использование пространства во всех файловых системах с активным управлением пространством и автоматически запускает пороговый перенос, когда процент используемого пространства в системе достигает верхнего порога или превышает его.

диалог (conversation)
Соединение между двумя программами в сеансе, который позволяет им взаимодействовать друг с другом при обработке транзакции.

динамическая сериализация (dynamic serialization)
Сериализация копий, при которой резервная или архивная копия файла или папки создается с первой попытки независимо от того, изменялись они во время резервного копирования или архивирования, или нет. Смотрите также разделяемая динамическая сериализация, разделяемая статическая сериализация, статическая сериализация.

домен (domain)
Группа клиентских узлов с одним или несколькими наборами политик управления данными и ресурсами системы хранения. Смотрите также домен политики.

домен клиента (client domain)
Набор выбранных пользователем накопителей, файловых систем или томов, для которых должно осуществляться резервное копирование или архивирование данных с использованием клиента резервного копирования и архивирования.

домен политики (policy domain)
Группа пользователей политики с одним или несколькими наборами политик, которые управляют ресурсами данных или ресурсами хранения для пользователей. Пользователи - это узлы-клиенты, связанные с доменом политики. Смотрите также активный набор правил политики, домен.

Ж

журнал восстановления (recovery log)
Журнал обновлений, которые предназначены для записи в базу данных. Журнал может служить для восстановления ошибок системы и носителей. Журнал восстановления состоит из активного журнала (включая зеркальную копию журнала) и архивных журналов.

журнал операций (activity log)
Журнал, в который записываются генерируемые сервером сообщения, связанные с его обычной работой. Эти сообщения включают данные об операциях сервера и клиента (например, время начала сеансов или ошибки ввода-вывода устройств).

журнал ошибок (error log)
Набор данных или файл, используемый для записи информации об ошибках продукта или системы.

З

задание переноса (migration job)
Спецификация файлов, которые нужно перенести, и действий, которые нужно выполнить с исходными файлами после переноса. Смотрите также файл задания, пороговый перенос.

задержка демонтирования (mount retention period)
Максимальное время в минутах, в течение которого сервер сохраняет неиспользуемый том на носителе с последовательным доступом, прежде чем размонтирует этот том на носителе с последовательным доступом.

закрытая регистрация (closed registration)
Процедура регистрации, при которой только администратору разрешено регистрировать рабочие станции в качестве клиентских узлов на сервере. Смотрите также открытая регистрация.

занятое логическое пространство (logical occupancy)
Пространство, занятое логическими файлами в пуле хранения. Это пространство не включает в себя неиспользуемое пространство, освобождающееся после удаления логических файлов из агрегатов, поэтому его объем может быть меньше, чем объем занятого физического пространства. Смотрите также занятое физическое пространство.

занятое физическое пространство (physical occupancy)
Пространство в пуле хранения, занятое физическими файлами. Это пространство включает в себя неиспользуемое пространство, создаваемое при удалении логических файлов из агрегатов. Смотрите также логический файл, занятое логическое пространство, физический файл.

запись в журнал на уровне предприятия (enterprise logging)
Процесс отправки событий с сервера на заданный сервер событий. Сервер событий направляет события назначенным получателям (например, обработчику пользователя). Смотрите также событие.

запись о событии (event record)
Запись базы данных, описывающая фактическое состояние и результаты событий.

защищенный сайт (protected site)

Смотрите первичный сайт.

зеркальное копирование (mirroring)

Процедура записи одних и тех же данных на несколько дисков одновременно. Зеркальное отображение данных позволяет защититься от потери данных в базе данных или в журнале восстановления.

И

идентификатор файлового пространства (file space ID, FSID)

Уникальный цифровой идентификатор, назначаемый сервером файловому пространству при его сохранении в серверном хранилище.

иерархия хранения (storage hierarchy)

Логический порядок первичных пулов хранения, заданный администратором. Обычно этот порядок определяется быстродействием и емкостью устройств, из которых состоят пулы хранения. Для формирования иерархии хранения нужно в определении каждого пула хранения указать следующий за ним пул. Смотрите также пул хранения.

именованный конвейер (named pipe)

Тип взаимодействий между процессами, который позволяет потокам данных сообщений передаваться от одного процесса-партнера к другому, например, от клиента к серверу и наоборот.

имя узла (node name)

Уникальное имя, обеспечивающее для сервера возможность идентификации рабочей станции, файл-сервера или персонального компьютера.

инкрементное резервное копирование (incremental backup)

Процесс резервного копирования файлов или каталогов или копирования страниц в базе данных, которые появились или изменились с момента последней операции полного или инкрементного резервного копирования. Смотрите также выборочное резервное копирование.

интерактивное резервное копирование тома (online volume backup)

Резервное копирование, при котором том остается доступным для других системных программ во время выполнения операции резервного копирования.

интерфейс прикладного программирования управления хранением данных (data storage-management application-programming interface, DSMAPI)

Набор функций и семантических правил, которые позволяют вести мониторинг событий файлов, а также управлять и манипулировать данными в файле. В среде HSM DSMAPI использует события для уведомления программ, управляющих данными, об операциях с файлами, сохраняет условную информацию об атрибутах для файла, поддерживает управляемые области в файле и применяет права доступа DSMAPI для управления доступом к объекту-файлу.

исключение (exclude)

Процесс идентификации файлов в списке включения-исключения. Этот процесс не дает производить резервное копирование или перенос файлов, когда пользователь или запланированное задание запускают операцию инкрементного или выборочного резервного копирования. Файл можно исключить из резервного копирования, из управления пространством или как из резервного копирования, так и из управления пространством.

использование ресурсов сеансом (session resource usage)

Время ожидания, процессорное время и пространство, используемое или освобожденное во время сеанса клиента.

исходная файловая система (originating file system)

Файловая система, из которой был перенесен файл. При возврате файла он возвращается в свою исходную файловую систему.

К

КБ (KB)

Смотрите килобайт.

квота (quota)

1. В случае HSM в системах AIX, UNIX или Linux: Предельный объем (в МБ) данных, который можно перенести или предварительно перенести из файловой системы в серверное хранилище.
2. В случае HSM в системах Windows: Заданный пользователем предельный объем пространства, занимаемый возвращенными файлами.

килобайт, КБ (kilobyte, KB)

В применении к процессорной памяти, реальной и виртуальной памяти и объему канала: два в 10-й степени или 1024 байт. В применении к дисковой памяти и объему информации при осуществлении взаимодействий: 1000 байт.

класс административных полномочий (administrative privilege class)

Смотрите класс полномочий.

класс полномочий (privilege class)

Уровень предоставленных администратору полномочий, Класс полномочий определяет, какие административные задачи может выполнять администратор. Смотрите также полномочия, класс полномочий узла, класс полномочий оператора, класс полномочий политики, класс полномочий хранения, класс системных полномочий.

класс полномочий оператора (operator privilege class)
Класс полномочий, позволяющий администратору отключать или останавливать сервер, включать сервер, отменять серверные процессы и управлять съемными носителями. Смотрите также класс полномочий.

класс полномочий политики (policy privilege class)
Класс полномочий, позволяющий администратору управлять объектами правил политики, регистрировать клиентские узлы и планировать для них клиентские операции. Эти полномочия могут ограничиваться определенными доменами политик. Смотрите также класс полномочий.

класс полномочий узла (node privilege class)
Класс полномочий, позволяющий администратору осуществлять удаленный доступ к клиентам резервного копирования и архивирования на отдельном клиентском узле или на всех клиентах в домене политики. Смотрите также класс полномочий.

класс полномочий хранения (storage privilege class)
Класс полномочий, предоставляющий администратору право управлять выделением и использованием ресурсов хранилища, в частности осуществлять мониторинг базы данных и журнала восстановления, а также серверного хранилища. Смотрите также класс полномочий.

класс системных полномочий (system privilege class)
Класс полномочий, предоставляющий администратору разрешение на выполнение всех команд сервера. Смотрите также класс полномочий.

класс управления (management class)
Объект политики, доступный для привязки к каждому файлу с целью указания способа серверного управления данным файлом. В классе управления может содержаться группа резервных копий, группа архивных копий и атрибуты управления пространством. Смотрите также привязка, группа копий, клиент управления иерархическим пространством, набор правил политики, пересвязать.

класс управления по умолчанию (default management class)
Класс управления, назначенный для набора политик. Этот класс используется для управления резервными копиями файлов и заархивированными файлами, если файл явным образом не связан ни с каким конкретным классом управления в списке включения-исключения.

класс устройства (device class)
Именованный набор характеристик, применяемых к группе устройств хранения. Каждый класс устройства имеет уникальное имя и представляет определенный тип устройства: диск, файл, оптический диск или лента.

клиент (client)
Программа или компьютер, который запрашивает доступ к службам на сервере. Смотрите также сервер.

клиент HSM (HSM client)
Смотрите клиент управления иерархическим пространством.

клиент администрирования (administrative client)
Программа, которая выполняется на файл-сервере, рабочей станции или мейнфрейме и при помощи которой администраторы управляют сервером и контролируют его. Смотрите также клиент резервного копирования и архивирования.

клиент библиотеки (library client)
Сервер, использующий обмен данными между серверами для доступа к библиотеке, которой управляет другой сервер управления хранением. Смотрите также менеджер библиотеки.

клиент резервного копирования-архивирования (backup-archive client)
Программа, которая работает на файловом сервере или рабочей станции и обеспечивает пользователям средства резервного копирования, архивирования, восстановления и получения файлов. Смотрите также клиент администрирования.

клиент/сервер (client/server)
Модель взаимодействия в распределенной обработке данных, в которой программа на одном компьютере отправляет требование, адресованное программе на другом компьютере и ожидает ответа. Программу, посылающую требование, называют клиентом, а отвечающую программу - сервером.

клиентский узел (client node)
Файл-сервер или рабочая станция, на которых установлена программа-клиент резервного копирования и архивирования и которые зарегистрированы на сервере.

клиентское приложение (application client)
Программа, установленная на компьютере для защиты программы. Сервер обеспечивает приложению-клиенту службы резервного копирования.

клиент управления иерархическим пространством (hierarchical storage management client, HSM client)
Программа-клиент, которая работает в сочетании с сервером, обеспечивая возможности управления иерархическим пространством (Hierarchical Storage Management - HSM) в системе. Смотрите также управление иерархическим пространством, класс управления.

командный сценарий IBM Spectrum Protect (IBM Spectrum Protect command script)
Последовательность административных команд IBM Spectrum Protect, которая хранится в базе данных сервера IBM Spectrum Protect. Сценарий можно запустить на сервере при помощи любого интерфейса. Сценарий может включать замену для параметров команд и условную логику. Смотрите также файл макрокоманд, сценарий.
контейнер (container)
Место хранения данных, например, файл, каталог или устройство. Смотрите также пул хранения контейнеров.
конфигурирование на уровне предприятия (enterprise configuration)
Метод настройки серверов, при котором администратор может дублировать конфигурацию одного из серверов на остальные серверы с использованием технологии взаимодействия серверов. Смотрите также менеджер конфигурации, управляемый сервер, профиль, подписка.
кэшировать (cache)
Сохранить идентичную копию файла на носителе с произвольным доступом при переносе файла в другой пул хранения в иерархии.

Л

ленточная библиотека (tape library)
Набор оборудования и средств, поддерживающий среду магнитных лент в установке. Ленточная библиотека может включать в себя стойки с устройствами хранения на магнитных лентах, механизмы автоматического монтирования лент, набор ленточных устройств и набор связанных ленточных томов, смонтированных на этих устройствах.
логический том (logical volume)
Часть физического тома, содержащая файловую систему.
логический файл (logical file)
Файл, хранящийся в одном или более пулах хранения либо в виде отдельного физического файла, либо в составе агрегата. Смотрите также агрегат, физический файл, занятое физическое пространство.
локальная сеть (local area network, LAN)
Сеть, которая соединяет друг с другом несколько устройств в ограниченном пространстве (например, в одном здании или университетском городке) и которая может соединяться с более крупной сетью.
локальный (local)

1. Относится к устройству, файлу или системе, доступ к которой осуществляется непосредственно с компьютера пользователя без использования линии связи.
2. Для продуктов по управлению иерархическим пространством: относящийся к пункту назначения перенесенных файлов, которые перемещаются. Смотрите также удаленный.

локальный теневой том (local shadow volume)
Данные, которые хранятся на теневых томах, находящихся в дисковой подсистеме хранения.
льготный период хранения архива (archive-retention grace period)
Время (в днях), в течение которого менеджер хранения будет хранить заархивированный файл, если серверу не удается повторно связать файл с соответствующим классом управления. Смотрите также привязка.
льготный период хранения резервных копий (backup retention grace period)
Срок (в днях), в течение которого будет хранить резервную версию, когда серверу не удается повторно связать файл с соответствующим классом управления.

М

максимальный размер блока передачи (maximum transmission unit, MTU)
Самый большой блок, который можно отправить на данный физический носитель в одном кадре. Например, максимальный размер блока передачи для Ethernet составляет 1500 байт.
МБ (MB)
Смотрите мегабайт.
мегабайт, МБ (megabyte, MB)
В применении к процессорной памяти, реальной и виртуальной памяти и объему канала: два в 20-й степени или 1 048 576 байт. В применении к дисковой памяти и объему информации при осуществлении взаимодействий: 1 000 000 байт.
медиа-сервер (media server)
В среде z/OS - программа, которая обеспечивает доступ к дисковой и ленточной системе хранения z/OS для серверов IBM Spectrum Protect, работающих в других операционных системах (не z/OS).
менеджер аварийного восстановления (disaster recovery manager, DRM)
Функция, позволяющая подготовить и использовать файл плана аварийного восстановления для сервера .
менеджер библиотеки (library manager)

Сервер, управляющий работой устройства хранения, которое совместно используется несколькими серверами управления хранением. Смотрите также клиент библиотеки.

менеджер конфигураций (configuration manager)
Сервер, который распространяет информацию о конфигурации, например, политики и расписания, на управляемые серверы в соответствии с их профилями. Информация о конфигурации может включать в себя политики и расписания. Смотрите также конфигурирование на уровне предприятия, управляемый сервер, профиль.

метаданные (metadata)
Данные, описывающие характеристики данных: описательные данные.

модуль plugin (plug-in)
Отдельно устанавливаемый программный модуль, который добавляет функцию в существующую программу, приложение или интерфейс.

моментальное восстановление VSS (VSS Instant Restore)
Операция, которая восстанавливает данные из локального снимка. Снимок - это резервная копия VSS, которая находится на локальном теневом томе. Операция восстановления получает данные, используя метод восстановления с помощью аппаратных средств (например, операция FlashCopy).

H

набор клиентских параметров (client option set)
Группа опций, заданных на сервере и используемых на клиентских узлах в сочетании с файлом опций клиента.

набор правил политики (policy set)
Группа правил в домене политики. Правила задают, как осуществляется автоматическое управление данными или ресурсами хранения для клиентских узлов в домене политики. Правила могут содержаться в классах управления. Смотрите также активный набор правил политики, класс управления.

набор резервных копий (backup set)
Переносимая консолидированная группа активных версий резервных копий файлов, сгенерированных для клиента резервного копирования и архивирования.

набор узлов GPFS (GPFS node set)
Смонтированная заданная группа файловых систем GPFS.

назначение (destination)
Атрибут группы копий или класса управления, задающий первичный пул хранения, в который будет выполняться резервное копирование, архивирование или перенастройка клиентского файла. Смотрите также пул хранения копий.

начальные данные (leader data)
Байты данных из начала перенесенного файла, которые сохраняются в файле остатка, соответствующем этому файлу в локальной файловой системе. Объем начальных данных, хранящихся в файле остатка, зависит от заданного размера файла остатка.

неактивная версия (inactive version)
Версия резервной копии файла, которая либо не является самой последней, либо относится к файлу, который больше не существует на клиентской системе. Неактивные версии резервных копий подлежат устареванию в соответствии с классом управления, назначенным для файла. Смотрите также активная версия, версия резервной копии.

неактивная файловая система (inactive file system)
Файловая система, для которой управление пространством было деактивировано. Смотрите также активная файловая система.

несвязанный стаб-файл (orphaned stub file)
Файл, для которого не удается найти перенесенный файл на сервере, с которым соединился клиентский узел для получения доступа к службам управления пространством. Например, стаб-файл может стать несвязанным, если вы модифицируете файл системных опций клиента, так чтобы соединяться не с тем сервером, на который был перенесен файл, а с каким-то другим сервером.

неструктурированный логический том (raw logical volume)
Часть физического тома, которая состоит из невыделенных блоков и для которой нет определения файловой системы JFS (journaled file system). Логический том доступен для чтения/записи только через низкоуровневые функции ввода-вывода.

нечеткая копия (fuzzy copy)
Резервная версия или архивная копия файла, которая может неточно отражать исходное содержимое этого файла из-за того, что во время резервного копирования или архивирования файла в файл вносились изменения.

нечеткая резервная копия (fuzzy backup)
Резервная версия файла, которая может не очень точно отражать текущее содержимое файла, поскольку в то время, как производилось резервное копирование файла, он подвергался модификации.

номер inode (inode number)
Номер, задающий конкретный файл индексного дескриптора файла в файловой системе.

номер логического устройства (logical unit number, LUN)
: В стандарте Small Computer System Interface (SCSI) - уникальный идентификатор, используемый для распознавания устройств, каждое из которых является логическим устройством (Logical Unit - LU).

О

область памяти (bucket)
: Облачный контейнер хранения, используемый Amazon Simple Storage Service (Amazon S3).

образ (image)
: Резервная копия файловой системы или неформатированного логического тома, созданная в виде единого объекта.

ограничение на монтирование (mount limit)
: Максимальное число томов одного класса, доступ к которым может осуществляться одновременно. Лимит монтирования определяет максимальное число точек монтирования. Смотрите также точка монтирования.

окно запуска (startup window)
: Период времени, в течение которого необходимо запустить расписание.

остаточный объект (tombstone object)
: Небольшое подмножество атрибутов удаленного объекта. Остаточный объект хранится в течение определенного срока, а в конце этого срока удаляется навсегда.

открытая регистрация (open registration)
: Процедура регистрации, при которой пользователи могут зарегистрировать на сервере свои рабочие станции в качестве клиентских узлов. Смотрите также закрытая регистрация.

П

пакет (packet)
: В связи для обмена данными: Последовательность двоичных разрядов, включая данные и управляющие сигналы, которые передаются и коммутируются как единое целое.

первичный пул хранения (primary storage pool)
: Именованный набор томов или контейнеров, используемых сервером для хранения резервных и архивных копий файлов, а также файлов, перенесенных с клиентских узлов. Смотрите также пул хранения копий, серверное хранилище, пул хранения, том пула хранения.

первичный узел (primary site)
: Физический или виртуальный узел, состоящий из аппаратных и сетевых ресурсов и ресурсов хранения. Обычно производственные операции выполняются на первичном узле. Данные можно реплицировать на вторичный узел для восстановления после аварии и передачи функций. Смотрите также вторичный узел.

передача данных в режиме без локальной сети (LAN-free data transfer)
: Смотрите перемещение данных в режиме без локальной сети.

перемещение данных в режиме без сети (LAN-free data movement)
: Перемещение данных между компьютером-клиентом и устройством хранения в сети хранения данных (SAN), в обход локальной сети.

перенесенный файл (migrated file)
: Файл, скопированный из локальной файловой системы в хранилище. В случае клиентов HSM в системах UNIX или Linux этот файл заменяется в локальной файловой системе на файл остатка. В системах Windows создание файла остатка необязательно. Смотрите также состояние файлов, предварительно перенесенный файл, резидентный файл, стаб-файл.

перенос (migrate)
: Перемещение данных в другое место или приложение в другой вычислительной системе.

перенос (migration)
: Процесс перемещения данных из одной вычислительной системы в другую или из приложения в другую вычислительную систему.

перенос по запросу (demand migration)
: Процесс, который используется, чтобы отреагировать на состояние переполнения пространства в файловой системе с активным управлением иерархическим пространством (Hierarchical Storage Management - HSM). Перенос файлов в серверное хранилище производится до тех пор, пока объем используемого пространства не упадет до нижнего порога, заданного для файловой системы. Если верхний и нижний порог совпадают, будет перенесен один файл. Смотрите также автоматический перенос, выборочный перенос, пороговый перенос.

пересвязать (rebind)
: Ассоциировать все версии резервных копий файла с новым именем класса управления. Например, файл, у которого есть активная версия резервной копии, пересвязывается, когда для более новой версии этого файла выполняется резервное копирование со связыванием с другим классом управления. Смотрите также привязка, класс управления.

период ожидания монтирования (mount wait period)
Максимальное время в минутах, в течение которого сервер ожидает выполнения запроса на монтирование тома с последовательным доступом, после чего отменяет запрос.
план аварийного восстановления (disaster recovery plan)
Файл, создаваемый менеджером аварийного восстановления (DRM) и содержащий сведения о восстановлении компьютерных систем в случае аварии и запускаемый для выполнения ряда задач восстановления. В частности, данный файл содержит сведения о программном и аппаратном обеспечении, используемом на сервере, и о местонахождении носителей, с которых должно производиться восстановление.
поврежденный файл (damaged file)
Физический файл, в котором были обнаружены ошибки чтения.
подписка (subscription)
В среде хранения: процесс идентификации подписчиков, среди которых распространяются профили. Смотрите также конфигурирование на уровне предприятия, управляемый сервер.
подтверждение (acknowledgment, ACK)
Передача символов подтверждения в качестве положительного ответа на передачу данных.
полное резервное копирование (full backup)
Процесс резервного копирования всей серверной базы данных. Операция полного резервного копирования начинает новую последовательность резервных копий базы данных. Смотрите также последовательность резервных копий базы данных, снимок базы данных, инкрементное резервное копирование.
полномочия (authority)
Право на доступ к объектам, ресурсам или функциям. Смотрите также класс полномочий.
получение (retrieve)
Копирование архивных данных из пула хранения на рабочую станцию для использования. При получении данных их архивная версия остается в пуле хранения. Смотрите также архивирование.
пользователь root (root user)
Системный пользователь, работающий без ограничений. У пользователя root есть специальные права и полномочия, необходимые для выполнения административных задач.
пороговый перенос (threshold migration)
Процесс перемещения файлов из локальной файловой системы в серверное хранилище, который производится на основе верхнего и нижнего порогов, заданных для файловой системы. Смотрите также автоматический перенос, перенос по запросу, задание переноса, выборочный перенос.
порог освобождения (reclamation threshold)
Процент пространства, которое должно иметься на томе носителя с последовательным доступом, чтобы сервер мог освободить этот том. Пространство становится доступным для освобождения с момента устаревания или удаления занимающих его файлов.
порог переноса (migration threshold)
Верхний и нижний пределы емкости (в процентах) для пулов хранения или файловых систем, при которых начинается или останавливается перенос.
последовательность резервных копий базы данных (database backup series)
Одна полная резервная копия базы данных и не более 32 инкрементных резервных копий, созданных с момента полного резервного копирования. Каждая операция полного резервного копирования начинает новую последовательность резервных копий базы данных. Число обозначает каждую последовательность резервных копий. Смотрите также снимок базы данных, полное резервное копирование.
правило авторизации (authorization rule)
Спецификация, разрешающая другому пользователю восстанавливать или получать файлы данного пользователя из хранилища .
правило аутентификации (authentication rule)
Спецификация, разрешающая другому пользователю восстанавливать или получать файлы из хранилища .
предварительно перенесенный файл (premigrated file)
Файл, который скопирован в серверное хранилище, но не заменен в локальной файловой системе на стаб-файл. В локальной файловой системе и в серверном хранилище находятся идентичные копии файла. Предварительно перенесенные файлы встречаются в файловых системах UNIX и Linux, в которые было добавлено управление пространством. Смотрите также состояние файлов, перенесенный файл, резидентный файл.
предварительный перенос (premigration)
Процесс копирования файлов, подлежащих переносу, в серверное хранилище, при котором исходные файлы в локальной файловой системе остаются без изменений.
префикс ленточного тома (tape volume prefix)
Высокоуровневый описатель имени файла или набора данных в стандартной метке ленты.
привязка (bind)
Привязать файл к имени класса управления. Смотрите также льготный период хранения архивов, класс управления, пересвязать.
приемник (receiver)

Серверный репозиторий, в котором содержится журнал с сообщениями сервера и клиентов в виде событий. Например, приемник может представлять собой обработчик файлов, обработчик пользователя или серверную консоль и журнал операций сервера. Смотрите также событие.

приемник клиента (client acceptor)
Служба, которая предоставляет Java-апплет веб-клиентам в веб-браузерах. В системах Windows Client Acceptor устанавливается и выполняется как служба. В системах AIX, UNIX и Linux client acceptor работает как демон.

примерная емкость (estimated capacity)
Доступное пространство пула хранения (в мегабайтах).

проверка (validate)
Проверка набора политик на наличие условий, которые могут вызвать проблемы при его переводе в активное состояние. Например, в процессе проверки выясняется, содержит ли набор политик класс управления по умолчанию.

прозрачный возврат (transparent recall)
Процесс, используемый для автоматического возврата перенесенного файла на рабочую станцию или на файл-сервер при осуществлении доступа к этому файлу. Смотрите также выборочный возврат.

пропускная способность (throughput)
В управлении хранением: Отношение общего числа байтов в рабочей нагрузке резервного копирования и восстановления (за исключением служебной нагрузки) к затраченному времени.

протокол связи (communication protocol)
Набор определений интерфейсов, который позволяет компьютерам взаимодействовать друг с другом.

профиль (profile)
Именованная группа сведений конфигурации, которая может распространяться менеджером конфигураций по подписке управляемого сервера. Информация о конфигурации может содержать ID зарегистрированных администраторов, политики, расписания клиентов, наборы опций клиента, административных расписания, командные сценарии менеджера хранения, определения серверов и определениях групп серверов. Смотрите также менеджер конфигурации, конфигурация на уровне предприятия, управляемый сервер.

процент предварительного переноса (premigration percentage)
Параметр управления пространством, который определяет, будет ли после порогового переноса или переноса по запросу производиться предварительный перенос очередных файлов-кандидатов на перенос.

пул активных данных (active-data pool)
Именованный набор томов хранения, содержащий только активные резервные версии клиентских данных. Смотрите также серверное хранилище, пул хранения, том пула хранения.

пул хранения (storage pool)
Набор томов или контейнеров хранения, которые служат пунктом назначения для хранения данных клиентов. Смотрите также пул активных данных, пул хранения облачных контейнеров, пул хранения копий, пул хранения каталогов-контейнеров, первичный пул хранения, иерархия хранения.

пул хранения каталога-контейнера (directory-container storage pool)
Пул хранения, используемый сервером для хранения данных в контейнерах в каталогах облачного пула. Данные, хранящиеся в пуле хранения каталогов-контейнеров, могут использовать либо встроенную дедупликацию данных, либо дедупликацию данных на стороне клиента. Смотрите также пул хранения облачных контейнеров, пул хранения контейнеров, пул хранения контейнеров-копий, пул хранения.

пул хранения контейнера-копии (container-copy storage pool)
Пул хранения, используемый сервером для хранения копий экстентов из пулов хранения каталогов-контейнеров. Эти копии используются для устранения повреждений в пуле хранения каталогов-контейнеров. Для пулов хранения контейнеров-копий используется носитель с последовательным доступом, такой как лента. Смотрите также пул хранения каталогов-контейнеров.

пул хранения контейнеров (container storage pool)
Первичный пул хранения, используемый сервером для хранения данных. Данные хранятся в контейнерах в каталогах файловой системы или в облачном хранилище. Если потребуется, производится дедупликация данных, когда сервер записывает их в пул хранения. Смотрите также пул хранения облачных контейнеров, контейнер, пул хранения каталогов-контейнеров.

пул хранения копий (copy storage pool)
Именованный набор томов, содержащих копии файлов из первичного пула хранения. Пулы хранения копий используются только для резервного копирования данных, находящихся в первичных пулах хранения. Пул хранения копий не может быть пунктом назначения для группы резервных копий или архивных копий, а также для класса управления (для перенесенных файлов). Смотрите также назначение, первичный пул хранения, серверное хранилище, пул хранения, том пула хранения.

пул хранения облачного контейнера (cloud-container storage pool)
Пул хранения, используемый сервером для хранения данных в облачном пространстве хранения. Облачное пространство хранения может находиться на месте или вне системы. Смотрите также пул хранения контейнеров, пул хранения каталогов-контейнеров, пул хранения.

путь (path)

Объект, определяющий отношение однозначную взаимосвязь между источником и пунктом назначения. Используя путь, источник получает доступ к пункту назначения. Данные могут передаваться от источника к месту назначения и в обратном направлении. Примером источника является средство перемещения данных (например, файл-сервер NAS), а примером пункта назначения - накопитель на магнитной ленте.

P

рабочая станция (workstation)
: Терминал или персональный компьютер, с которого пользователь может запускать программы; обычно подсоединен к мэйнфрэйму или к сети.

раздел (stanza)
: Группа строк в файле, которые вместе несут общую функцию или задают часть системы. Разделы обычно разделяются пустыми строками или двоеточиями, и у каждого раздела есть имя.

раздел рабочей нагрузки (workload partition, WPAR)
: Раздел в пределах одного экземпляра операционной системы.

разделяемая динамическая сериализация (shared dynamic serialization)
: Значение сериализации, указывающее на недоступность создания резервной или архивной копии файла, если он изменяется во время операции. Клиент резервного копирования и архивирования несколько раз попытается повторить операцию резервного копирования или архивирования; если окажется, что файл изменялся во время каждой из попыток, то при последней попытке клиент резервного копирования и архивирования произведет резервное копирование или архивирование этого файла. Смотрите также динамическая сериализация, сериализация, разделяемая статическая сериализация, статическая сериализация.

разделяемая статическая сериализация (shared static serialization)
: Значение сериализации группы копий, которое указывает, что во время резервного копирования или архивирования файл не должен изменяться. Клиент предпримет несколько попыток выполнить операцию. Если окажется, что файл использовался при каждой попытке, операция резервного копирования или архивирования не производится. Смотрите также динамическая сериализация, сериализация, разделяемая динамическая сериализация, статическая сериализация.

размер стаб-файла (stub file size)
: Размер файла, который заменит исходный файл в локальной файловой системе при его переносе в серверное хранилище. Размер, заданный для файлов остатков, определяет, сколько начальных данных может сохраняться в файле остатка. По умолчанию размер файла остатка равен размеру блока, заданному для файловой системы, минус 1 байт.

разреженный файл (sparse file)
: Файл, созданный с длиной, которая превышает длину содержащихся в нем данных; при этом в нем остается пустое пространство для последующего добавления данных.

рандомизация (randomization)
: Процесс распространения запланированного времени запуска для различных клиентов в рамках заданного процентного отношения окна запуска расписания.

расписание (schedule)
: Запись в базе данных, которая описывает запланированные операции клиента или административные команды, которые нужно обработать, и содержащая расписание их выполнения. Смотрите также запланированное административное задание, расписание клиента.

расписание выполнения административных команд (administrative command schedule)
: Запись базы данных, описывающая плановое выполнение административной команды в течение указанного временного периода. Смотрите также централизованный планировщик, расписание клиента, расписание.

расписание клиента (client schedule)
: Запись базы данных, описывающая плановое выполнение клиентских операций в течение указанного временного периода. К клиентским операциям относятся: резервное копирование, архивирование, восстановление (или получение), а также команда клиентской операционной системы (макрокоманда). Смотрите также запланированное административное задание, централизованный планировщик, расписание.

расширение (extend)
: Увеличение части доступного пространства, отведенной для хранения базы данных или журнала восстановления.

расширенный атрибут (Extended Attribute, EA)
: Имена пар имен или значений, связанные с файлами или каталогами. Существует три класса расширенных атрибутов: пользовательские атрибуты, системные атрибуты и доверенные атрибуты.

регистрировать (register)
: Задать клиентский узел или ID администратора, который может получать доступ к серверу.

реестр (registry)
: Репозиторий, в котором содержится информация по управлению доступом и по конфигурированию для пользователей, систем и программ.

режим (mode)

Атрибут группы копий, который указывает, нужно ли создавать резервную копию файла, который не изменился с момента создания последней резервной копии. Смотрите также абсолютный режим, режим измененных файлов.

режим доступа (access mode)
Атрибут пула хранения или тома хранения, указывающий на возможность чтения сервером сведений пула хранения или тома хранения или запись в них.

режим измененных файлов (modified mode)
В управлении пространством: Режим группы резервных копий, при котором файл или каталог подлежит инкрементному резервному копированию, только если он изменился с момента создания его последней резервной копии. Считается, что файл или каталог изменился, если изменились дата, размер, владелец файла или разрешения на доступ к этому файлу. Смотрите также абсолютный режим, режим.

режим планирования по запросам сервера (server-prompted scheduling mode)
Способ взаимодействия клиента с сервером, при котором сервер связывается с клиентским узлом, когда нужно выполнить какие-либо задачи. Смотрите также режим планировщика с опросом клиента.

режим планировщика (scheduling mode)
Тип операций планирования на узле клиента и сервера, обеспечивающий поддержку двух режимов планирования: опрос клиентов и подсказка сервера.

режим планировщика с опросом клиента (client-polling scheduling mode)
Метод работы, при котором клиент запрашивает у сервера информацию о подлежащих выполнению операциях. Смотрите также режим планирования по запросам сервера.

режим частичного возврата файла (partial-file recall mode)
Режим возврата, при котором функция управления иерархическим пространством (Hierarchical Storage Management - HSM) читает из хранилища только часть перенесенного файла, затребованную программой, которое обратилось к этому файлу.

резервная версия (backup version)
Файл или каталог, резервную копию которого узел-клиент создал в хранилище. В хранилище может существовать несколько резервных версий, но активной версией является только одна из них. Смотрите также активная версия, группа копий, неактивная версия.

резервное копирование VSS (VSS Backup)
Операция резервного копирования, при выполнении которой используется технология Microsoft Volume Shadow Copy Service (VSS). Операция резервного копирования генерирует онлайновый снимок (непротиворечивую копию на определенный момент времени). Эту копию можно сохранить на локальных теневых томах или в серверном хранилище.

резервное копирование VSS с выгрузкой (VSS offloaded backup)
Операция резервного копирования, которая использует аппаратного провайдера Microsoft Volume Shadow Copy Service (VSS) (установленного в другой системе) для перемещения данных на сервер. Этот тип операций резервного копирования позволяет перераспределить нагрузку, связанную с резервным копированием, из производственной системы в другую систему.

резервное копирование в режиме копирования (copy backup)
Полное резервное копирование, при котором файлы журнала транзакций не удаляются, так чтобы не препятствовать выполнению процедур резервного копирования с использованием инкрементного или дифференциального резервного копирования.

резервное копирование группы (group backup)
Создание резервной копии группы, содержащей список файлов из одного или нескольких исходных файловых пространств.

резервное копирование логического тома (logical volume backup)
Процесс копирования файловой системы или логического тома как единого объекта.

резервное копирование на основе журнала (journal-based backup)
Метод резервного копирования для клиентов Windows и клиентов AIX, которые используют механизм уведомления об изменениях в файлах, чтобы повысить производительность инкрементного резервного копирования за счет сокращения числа операций полного сканирования файловой системы.

резервное копирование образа (image backup)
Резервное копирование всей файловой системы или пустого логического тома как единого объекта.

резидентный файл (resident file)
В системе Windows: Полный файл в локальной файловой системе, который может быть также и перенесенным файлом, так как в серверном хранилище может существовать перенесенная копия. В системе UNIX или Linux: Полный файл в локальной файловой системе, который не подвергался ни переносу, ни предварительному переносу, либо был возвращен из серверного хранилища и изменен.

С

связи профиля (profile association)

В менеджере конфигурации: заданное взаимоотношение между профилем и таким объектом, как домен политики. Профилем определяется конфигурационная информация, которая будет передаваться управляемому серверу, когда он подпишется на этот профиль.

сеанс (session)
Логическое или виртуальное соединение между двумя станциями, программами или устройствами в сети, которое позволяет двум элементам взаимодействовать друг с другом и обмениваться данными в течение сеанса. Смотрите также административный сеанс.

сеанс администратора (administrative session)
Период времени, в течение которого процесс с пользовательским идентификатором администратора взаимодействует с сервером для выполнения административных задач. Смотрите также сеанс клиентского узла, сеанс.

сеанс работы клиентского узла (client node session)
Сеанс, в течение которого клиентский узел взаимодействует с сервером для выполнения запросов на резервное копирование, восстановление, архивирование, получение, перенос или возврат файлов. Смотрите также административный сеанс.

сервер (server)
Программа или компьютер, предоставляющие службы другим программам или компьютерам. Смотрите также клиент.

сервер менеджера данных (data manager server)
Сервер, который собирает информацию о метаданных для инвентаризации клиента и управляет выполнением транзакций для агента хранения по локальной сети. Сервер менеджера данных сообщает агенту хранения информацию о применимых атрибутах библиотеки и идентификатор тома назначения.

сервер событий (event server)
Сервер, на который другие серверы пересылают события для записи в журнал. Сервер событий перенаправляет события на приемники, на которых включена отправка событий сервера.

сериализация (serialization)
Процесс обработки файлов, измененных в ходе выполнения резервного копирования или архивирования. Смотрите также разделяемая динамическая сериализация, разделяемая статическая сериализация, статическая сериализация.

сеть хранения данных (SAN)
Выделенная сеть хранения данных, настроенная в соответствии с особенностями данной среды и объединяющая в себе серверы, компьютеры, продукты для управления хранением данных, сетевые продукты, программы и службы.

сжатие (compression)
Функция, которая удаляет повторяющиеся символы, пробелы, строки символов или двоичные данные из обрабатываемых данных и заменяет символы управляющими символами. Сжатие позволяет уменьшить объем пространства, необходимый для хранения данных. Смотрите также встроенное сжатие.

символ подстановки (wildcard character)
Специальный символ, такой как звездочка (*) или знак вопроса (?), который можно использовать для представления одного или нескольких символов. Символ подстановки может обозначать любой символ или набор символов.

символ шаблона вхождений (pattern-matching character)
Смотрите: символ подстановки.

склад данных (data store)
В виртуализованной среде: расположение, в котором хранятся данные виртуальной машины.

скорость передачи данных по сети (network data-transfer rate)
Скорость, определенная путем деления общего числа переданных байт на время передачи данных. Например, этот показатель может определяться временем, затраченным на передачу данных по сети.

служба журнала (journal service)
В Microsoft Windows: Программа, которая следит за активностью файлов, находящихся в файловых системах.

снимок (snapshot)
Тип резервного копирования образа, позволяющий получить просмотр тома в отдельный момент времени.

снимок базы данных (database snapshot)
Полная резервная копия всей базы данных на съемном носителе, который можно переместить за пределы локального сайта. При создании снимка базы данных текущая последовательность резервных копий базы данных не нарушается. Со снимком базы данных не могут быть связаны инкрементные резервные копии. Смотрите также последовательность резервных копий базы данных, полное резервное копирование.

собрание наборов резервных копий (backup set collection)
Группа одновременно созданных наборов резервных копий с одним и тем же именем набора резервных копий, описание, а также с одними и теми же именами томов и классами устройств. Сервер идентифицирует каждый набор резервных копий в собрании по имени узла, имени набора резервных копий и типу файла.

собственная файловая система (native file system)

Файловая система, которая локальным образом добавленная на файл-сервер, но в которую не добавлено управление пространством. Клиент HSM (Hierarchical Storage Manager) не предоставляет служб управления пространством для такой файловой системы.

событие (event)

Существенное происшествие, касающееся задачи или системы. К событиям могут относится завершение или неудачное завершение операции, действие пользователя или изменение состояния процесса. Смотрите также запись в журнал на уровне предприятия, приемник.

совместное размещение (collocation)

Процесс размещения всех данных, относящихся к файловому пространству одного клиента, клиентскому узлу или к группе клиентских узлов на минимальном числе томов с последовательным доступом в пуле хранения. При совместном размещении можно сократить число томов, к которым придется обращаться при восстановлении больших объемов данных.

совместно используемая библиотека (shared library)

Устройство библиотеки, используемое несколькими серверами управления хранением.

согласование (reconciliation)

Процесс, позволяющий обеспечить непротиворечивость между исходным репозиторием данных и более крупной системой, в которой хранятся данные для резервного копирования. Примерами более крупных систем, в которых хранятся данные для резервного копирования, являются серверы хранения или другие системы хранения. В процессе согласования данные, которые, как было установлено, больше не нужны, удаляются.

состояние файла (file state)

Режим управления пространством для файла, находящегося в файловой системе, в которую было добавлено управление хранением данных. Файл может находиться в одном из трех состояний: резидентном, предварительно перенесенном или перенесенном. Смотрите также перенесенный файл, предварительно перенесенный файл, резидентный файл.

состояние файловой системы (file system state)

Режим управления пространством в файловой системе, которая находится на рабочей станции, на которой установлен клиент управления иерархическим пространством (Hierarchical Storage Management - HSM). Возможные состояния файловой системы: нативное, активное, неактивное и глобально неактивное.

специальный файл (special file)

В системах AIX, UNIX или Linux: Файл, который задает устройства для системы, или временные файлы, создаваемые процессами. Существует три основных типа специальных файлов: FIFO (first-in, first-out), блочные и символьные.

список include-exclude (include-exclude list)

Список опций, которые позволяют включать файлы в операции резервного копирования и исключать их из этих операций. Опция exclude указывает, для каких файлов не следует производить резервное копирование. Опция include задает файлы, на которые не распространяются общие правила исключения, или назначает для файла или для группы файлов класс управления для служб резервного копирования или архивирования. Смотрите также файл включения-исключения.

список исключения-включения (exclude-include list)

Смотрите список включения-исключения.

список управления доступом (access control list, ACL)

В компьютерной защите: Связанный с объектом список, где указаны все субъекты, которым разрешен доступ к объекту, и их права доступа.

способ связи (communication method)

Способ, посредством которого клиент и сервер обмениваются информацией. Смотрите также Transmission Control Protocol/Internet Protocol.

срок хранения (retention)

Время (в днях), по истечении которого неактивные резервные или архивные копии файлов удаляются из пула хранения. Срок хранения определяется атрибутами группы копий и отсрочкой хранения по умолчанию для домена.

стаб (stub)

Ярлык в файловой системе Windows, генерируемый клиентом управления иерархическим пространством (Hierarchical Storage Management - HSM) для перенесенного файла, чтобы обеспечить возможность прозрачного доступа к этому файлу. Остаток - это представление перенесенного файла в виде разреженного файла, к которому присоединена точка пересмотра.

стабилизационное файловое пространство (stabilized file space)

Файловое пространство, которое существует на сервере, но не на клиенте.

стаб-файл (stub file)

Файл, которым в локальной файловой системе заменяется исходный файл после его переноса в систему хранения. В стаб-файле содержится информация, необходимая для возврата перенесенного файла из серверного хранилища. В нем также содержится дополнительная информация, при использовании которой возврат перенесенного файла может и не понадобиться. Смотрите также перенесенный файл, резидентный файл.

статическая сериализация (static serialization)

Значение сериализации группы копий, которое указывает, что во время резервного копирования или архивирования файл не должен изменяться. Если окажется, что файл использовался во время первой попытки, клиент резервного копирования и архивирования не сможет выполнить операцию резервного копирования или архивирования. Смотрите также динамическая сериализация, сериализация, разделяемая динамическая сериализация, разделяемая статическая сериализация.

страница (page)
Заданная единица пространства на носителе хранения или на томе базы данных.

суммарная скорость передачи данных (aggregate data transfer rate)
Статистический показатель производительности, представляющий собой среднее число байт, передаваемых в секунду при обработке данной операции.

сценарий (script)
Ряд собранных в файле, команд, которые при запуске файла выполняют определенную функцию. Сценарии интерпретируются во время их выполнения. Смотрите также командный сценарий IBM Spectrum Protect.

Т

тайм-аут (timeout)
Интервал времени, отведенный для завершения события или для выполнения определенных операций, прежде чем они будут прерваны.

теневая копия (shadow copy)
Снимок тома. Снимок можно сделать, пока приложения в системе продолжают записывать данные на тома.

теневой том (shadow volume)
Данные, сохраненные из снимка тома. Снимок можно сделать, пока приложения в системе продолжают записывать данные на тома.

тип устройств File (file device type)
Тип устройств, который задает использование файлов с последовательным доступом в дисковом пространстве хранения в виде томов.

том (volume)
Дискретный блок пространства хранения на диске, магнитной ленте или другом носителе для записи данных который поддерживает идентификатор того или иного вида и список таких параметров, как метка тома или управление вводом-выводом. Смотрите также чистый том, серверное хранилище, пул хранения, том пула хранения.

том пула хранения (storage pool volume)
Том, назначенный пулу хранения. Смотрите также пул активных данных, пул хранения копий, первичный пул хранения, серверное хранилище, том.

точка монтирования (mount point)
Логический диск, через который осуществляется доступ к томам в классе устройств с последовательным доступом. В случае типов устройств со сменными носителями (например, магнитной ленты) точка монтирования представляет собой логический диск, связанный с физическим накопителем. В случае устройств файлового типа точка монтирования представляет собой логический диск, связанный с потоком ввода-вывода. Смотрите также лимит монтирования.

точка принятия (commit point)
Момент времени, когда данные считаются непротиворечивыми.

У

удаление дубликатов (deduplication)
Смотрите дедупликация данных.

удаленный (remote)
Для продуктов по управлению иерархическим пространством: относящийся к источнику перенесенных файлов, которые перемещаются. Смотрите также локальный.

узел NAS (NAS node)
Клиентский узел, являющийся файл-сервером NAS. Данные для узла NAS передаются файл-сервером NAS, который управляется протоколом NDMP (Network Data Management Protocol). Узел NAS иначе называется узлом файл-сервера NAS.

узел (node)
Файл-сервер или рабочая станция, на которых установлена программа-клиент резервного копирования и архивирования и которые зарегистрированы на сервере.

узел агента (agent node)
Клиентский узел, которому предоставлено прокси-разрешение на выполнение операций от имени другого клиентского узла, выступающего в качестве узла назначения.

узел восстановления (recovery site)
Смотрите вторичный сайт.

узел назначения (target node)
: Клиентский узел, являющийся объектом прокси-разрешения для других клиентских узлов (именуемых узлами агентов). Прокси-разрешение позволяет узлам-агентам выполнять операции с данными (например, резервное копирование и восстановление) от имени узла назначения.

узел файл-сервера NAS (NAS file server node)
: Смотрите узел NAS.

управление жизненным циклом информации (information lifecycle management, ILM)
: Система управления файлами на основе политики для пулов хранения и наборов файлов. Смотрите также General Parallel File System.

управление иерархическим пространством (hierarchical storage management - HSM)
: Функция, которая автоматически распределяет данные и управляет данными на диске и/или на магнитной ленте, относя устройства этих типов и, потенциально, другие устройства в разным уровням в иерархии хранения, начиная от быстрых дорогостоящих устройств и заканчивая более медленными дешевыми устройствами (возможно, со сменными носителями. Ее назначение - свести к минимум время доступа к данным и максимально использовать доступную емкость носителей. Смотрите также клиент управления иерархическим пространством, возврат, иерархия хранения.

управление пространством (space management)
: Смотрите управление иерархическим пространством.

управляемый объект (managed object)
: Определение в базе данных управляемого сервера, которое менеджер конфигурации распространил на управляемый сервер. Когда управляемый сервер подписывается на профиль, все объекты, связанные с этим профилем, становятся управляемыми объектами в базе данных управляемого сервера.

управляемый сервер (managed server)
: Сервер, который получает сведения о конфигурации от менеджера конфигурации путем подписки на один или несколько профилей. Сведения о конфигурации могут включать определения таких объектов, как политика и расписания. Смотрите также менеджер конфигурации, конфигурация на уровне предприятия, профиль, подписка.

устаревание (expiration)
: Процесс идентификации файлов, наборов данных или объектов, которые подлежат удалению, поскольку истек срок их действия или закончился срок их хранения.

устаревший файл (expiring file)
: Перенесенный или предварительно перенесенный файл, помеченный как устаревший для удаления из системы хранения. Если из локальной файловой системы удаляется файл остатка или исходная копия предварительно перенесенного файла либо если обновляется исходная копия предварительно перенесенного файла, во время очередной операции согласования соответствующий перенесенный или предварительно перенесенный файл помечается как устаревший.

устройство перемещения данных (data mover)
: Устройство, производящее перемещение данных от имени сервера. Данные перемещает файл-сервер NAS (Network-Attached Storage).

Ф

файл включения-исключения (include-exclude file)
: Файл, содержащий операторы, которые определяют, какие файлы подлежат резервному копированию, и задают связанные классы управления для резервных или архивных копий. Смотрите также список включения-исключения.

файл задания (job file)
: Сгенерированный файл, содержащий информацию о конфигурации для задания по переносу. Этот файл представлен в формате XML, и его можно создавать и редактировать при помощи графического пользовательского интерфейса клиента HSM (hierarchical storage management) для Windows. Смотрите также задание по переносу.

файл конфигурации устройств (device configuration file)
: 1. В случае сервера: Файл, содержащий информацию о заданных классах устройств, и, на некоторых серверах, о заданных библиотеках и устройствах. Эти сведения представляют собой копию сведений о конфигурации устройств в базе данных.
2. В случае агента хранения: Файл, содержащий имя и пароль агента хранения и информацию о сервере, который управляет подключенными к SAN библиотеками и дисками, используемыми агентом хранения.

файл кэша (cache file)
: Снимок логического тома, создаваемый агентом Logical Volume Snapshot Agent (LVSA). Во время резервного копирования образа блоки сохраняются сразу после их изменения, и их логические экстенты сохраняются в файлах кэша.

файл макрокоманд (macro file)

Файл, который содержит одну или несколько административных команды IBM Spectrum Protect, которые можно выполнять только с клиента администрирования с помощью команды MACRO. Смотрите также командный сценарий IBM Spectrum Protect.

файловое пространство (file space)
Логическое пространство в системе хранения сервера, содержащее группу резервных или архивных копий файлов, созданных клиентским узлом с одного логического раздела, из одной файловой системы или из одной виртуальной точки монтирования. Клиентские узлы могут восстанавливать, получать и удалять свои файловые пространства из серверного хранилища . В серверном хранилище файлы, относящиеся к одному и тому же файловому пространству, могут храниться не вместе.

файловое пространство Unicode (Unicode-enabled file space)
Файловое пространство, имя которого соответствует стандарту Unicode и совместимо с любой локалью на рабочих станциях с несколькими языками.

файл опций (options file)
Файл, содержащий опции обработки. Смотрите также файл системных опций клиента, файл пользовательских опций клиента.

файл опций клиента (client options file)
Редактируемый файл, в котором указан сервер и способ связи, а также содержатся параметры конфигурации для резервного копирования, архивирования, управления иерархическим пространством (HSM) и планирования.

файл опций сервера (server options file)
Файл, содержащий параметры, которые управляют различными операциями сервера. Эти параметры определяют такие свойства, как связь, устройства и производительность.

файл пользовательских опций клиента (client user-options file)
Файл, содержащий набор опций обработки, используемый клиентами в системе. Этот набор может содержать опции, которые определяют, с каким сервером соединяется клиент, а также опции, влияющие на операции резервного копирования, архивирования, управления иерархическим пространством, а также на запланированные операции. Это файл носит имя dsm.opt. В случае систем AIX, UNIX или Linux смотрите также файл системных опций клиента. Смотрите также файл системных опций клиента, файл опций.

файл-сервер (file server)
Специально выделенный компьютер и его периферийные устройства хранения данных, соединенные с локальной сетью, где хранятся программы и файлы, с которыми совместно работают пользователи в сети.

файл-сервер NAS (NAS file server)
Смотрите файл-сервер Network-Attached Storage.

файл-сервер Network-Attached Storage (Network-Attached Storage file server)
Выделенное устройство хранения данных с операционной системой, оптимизированной под выполнение функций обслуживания файлов. Файл-сервер NAS может одновременно обладать характеристиками узла и устройства перемещения данных.

файл системных опций клиента (client system-options file)
Файл, который используется на клиентах в системах AIX, UNIX и Linux и содержит набор опций обработки, указывающих, к каким серверам нужно обращаться для получения доступа к службам. Этот файл также задает способы связи и параметры резервного копирования, архивирования, управления иерархическим пространством и планирования. Смотрите также файл пользовательских опций клиента, файл опций.

файл с управлением пространством (space-managed file)
Файл, перенесенный с клиентского узла клиентом управления иерархическим хранением (клиентом HSM). Клиент HSM возвращает файл на клиентский узел по требованию.

файл хронологии тома (volume history file)
Файл, содержащий информацию о томах, использовавшихся сервером для резервных копий и базы данных и для экспорта данных об администраторах, узлах, правилах политики или серверах. В этом файле также содержится информация о томах пулов хранения с последовательным доступом, которые были добавлены, повторно использованы или удалены. Эта информация представляет собой копию информации о томе, записанной в базе данных сервера.

физический файл (physical file)
Файл, непосредственно хранящийся в одном или более пулах хранения и состоящий из одного логического файла либо нескольких логических файлов, объединенных в агрегат. Смотрите также агрегат, логический файл, занятое физическое пространство.

X

хранилище сервера (server storage)
Первичные пулы хранения, пулы хранения копий и пулы хранения активных данных, которые используются сервером для хранения таких файлов пользователей, как версии резервных копий, архивные копии и файлы, перенесенные с узлов-клиентов управления пространством (файлы с управлением пространством). Смотрите

также пул активных данных, пул хранения контейнеров, пул хранения копий, первичный пул хранения, том пула хранения, том.

Ц

централизованный планировщик (central scheduler)
: Функция, позволяющая администратору планировать выполнение клиентских операций и административных команд. Операции можно запланировать, так чтобы они выполнялись периодически или в заданный день. Смотрите также запланированное административное задание, расписание клиента.

центр данных (data center)
: В виртуализованной среде: контейнер, в котором находятся хосты, кластеры, сети и склады данных.

Ч

частота (frequency)
: Атрибут группы копий, который задает минимальный интервал (в днях) между операциями инкрементного резервного копирования.

чистый том (scratch volume)
: Том, у которого есть метка и который либо пуст, либо не содержит допустимых данных и при этом не задан и доступен для использования. Смотрите также том.

Э

ЭБ (EB)
: Смотрите экзабайт.

экзабайт, ЭБ (exabyte, EB)
: В применении к процессорной памяти, реальной и виртуальной емкости хранения и объему канала: два в 60-й степени или 1 152 921 504 606 846 976 байт. В применении к дисковой памяти и объему информации при осуществлении взаимодействий: 1 000 000 000 000 000 000 байт.

экстент (extent)
: Часть файла, созданная в процессе дедупликации данных. Экстенты сравниваются с экстентами других файлов с целью идентификации дубликатов.