IBM Spectrum Protect
версия 8.1.7

Руководство по дисковому решению с несколькими площадками

IBM Spectrum Protect
версия 8.1.7

Руководство по дисковому решению с несколькими площадками

Примечание:
Прежде чем использовать эту информацию и описываемый в ней продукт, прочтите информацию в разделе “Замечания” на стр. 181.

Данное издание относится к версии 8, выпуску 1, модификации 7 IBM Spectrum Protect (номера продукта 5725-W98, 5725-W99, 5725-X15) и ко всем его последующим выпускам и модификациям, пока в новых изданиях не будет указано иное.

Содержание

Об этой публикации v
Для кого предназначено это руководство v
Публикации v

Что нового в этом выпуске vii

Часть 1. Планирование дискового решения по защите данных с несколькими площадками 1

Глава 1. Выбор размера системы . . . 3

Глава 2. Планирование площадок . . . 5

Глава 3. Требования к системе для дискового решения с несколькими площадками 9
Требования к аппаратным средствам 9
Требования к программному обеспечению 11

Глава 4. Рабочие листы планирования 15

Глава 5. Планирование хранения . . . 27
Планирование массивов хранения 27

Глава 6. Планирование защиты. . . . 31
Планирование ролей администратора 31
Планирование защищенной связи 32
Планирование хранения зашифрованных данных . . 33
Планирование доступа через брандмауэр 33

Часть 2. Реализация решения по защите данных на диске для нескольких площадок 37

Глава 7. Настройка системы 39
Конфигурирование оборудования систем хранения 39
Установка операционной системы сервера 39
Установка в системах AIX. 40
Установка в системах Linux 41
Установка в системах Windows 46
Конфигурирование ввода-вывода с несколькими путями 46
Системы AIX 47
Системы Linux 48
Системы Windows 49
Создание ID пользователя для сервера 50
Подготовка файловых систем для сервера 51
Системы AIX 51
Системы Linux 52
Системы Windows 53

Глава 8. Установка сервера и компонента Центр операций 55
Установка в системах AIX и Linux 55
Установка обязательных файлов RPM для графического мастера 56
Установка в системах Windows 56

Глава 9. Конфигурирование сервера и компонента Центр операций 59
Конфигурирование экземпляра сервера 59
Установка клиента резервного копирования и архивирования 60
Как задать опции для сервера 61
Конфигурирование защищенной связи с использованием Transport Layer Security (TLS) . . . 62
Конфигурирование Центра операций 63
Защита связи между компонентом Центр операций и хаб-сервером 63
Регистрация лицензии на продукт 66
Конфигурирование дедупликации данных 66
Как задать правила хранения данных для вашего бизнеса 67
Как задать расписания для операций по обслуживанию сервера 67
Определение расписаний клиентов 70

Глава 10. Установка и конфигурирование клиентов резервного копирования и архивирования 71
Регистрация и назначение клиентов в расписания . . 71
Установка службы управления клиентом 72
Проверка того, правильно ли установлена служба управления клиентами 73
Конфигурирование Центр операций на использование службы управления клиентом . . 74

Глава 11. Конфигурирование второго сервера 77
Конфигурирование связи SSL между хаб-сервером и подчиненным сервером 77
Добавление второго сервера как подчиненного сервера 79
Как включить репликацию 79

Глава 12. Завершение реализации . . 81

Часть 3. Мониторинг дискового решения с несколькими площадками 83

Глава 13. Контрольный список ежедневного мониторинга. 85

Глава 14. Контрольный список периодического мониторинга 95

Глава 15. Проверка на соответствие лицензии 103

Глава 16. Состояние системы отслеживания с использованием отчетов по электронной почте . . . 105

Часть 4. Управление операциями для дискового решения с несколькими площадками 107

Глава 17. Управление Центром операций 109
Добавление и удаление подчиненных серверов . . . 109
Добавление подчиненного сервера 109
Удаление подчиненного сервера 110
Запуск и остановка веб-сервера 111
Перезапуск мастера начального конфигурирования 111
Изменение хаб-сервера 112
Восстановление конфигурации до предварительно сконфигурированного состояния 113

Глава 18. Защита приложений, виртуальных машин и компьютеров . 115
Добавление клиентов 115
Выбор программного обеспечения клиента и планирование установки 116
Как задать роли для резервного копирования и архивирования данных клиента 118
Планирование операций резервного копирования и архивирования 121
Регистрация клиентов. 122
Установка и настройка клиентов 123
Управление операциями клиентов. 129
Оценка ошибок в журналах ошибок клиентов . . 129
Остановка и перезапуск приемника клиента. . . 130
Изменение паролей 131
Изменение объема резервного копирования клиента 132
Управление обновлениями клиентов 133
Списание клиентского узла 134
Деактивация данных для высвобождения пространства хранения 137

Глава 19. Управление хранилищем данных 139
Аудит контейнера пула хранения 139
Управление емкостью перечня 140
Управление использованием памяти и процессора 142
Тонкая настройка запланированных операций . . . 143
Перемещение клиентов с одного сервера на другой. 144

Глава 20. Управление репликацией 147
Совместимость репликации 147
Как включить репликацию узлов 147
Защита данных в пулах хранения каталогов-контейнеров 148
Изменение параметров репликации 150
Как задать разные политики сохранения для исходного сервера и целевого сервера 151

Глава 21. Защита сервера. 153
Понятия, касающиеся защиты 153
Управление администраторами 156
Изменение требований к паролям 157
Защита IBM Spectrum Protect в системе 158
Ограничение доступа пользователей к серверу 158
Ограничение доступа путем ограничений портов 159

Глава 22. Остановка и запуск сервера 161
Остановка сервера 161
Запуск сервера для задач обслуживания или реконфигурирования 162

Глава 23. Планирование обновления сервера 165

Глава 24. Подготовка к отключению или обновлению системы 167

Глава 25. Реализация плана аварийного восстановления 169
Выполнение отработки восстановления 169

Глава 26. Восстановление после потери данных или системных отключений электричества. 171
Восстановление базы данных 173
Восстановление поврежденных данных от реплицированной копии 175
Исправление пулов хранения данных 176

Часть 5. Приложения 177

Приложение. Специальные возможности для семейства продуктов IBM Spectrum Protect. . . 179

Замечания 181

Глоссарий 187

Индекс 189

Об этой публикации

В этой публикации представлена информация о планировании, реализации, мониторинге и работе с решением по защите данных, в котором используются наилучшие практические методы IBM Spectrum Protect.

Для кого предназначено это руководство

Это руководство предназначено для всех пользователей, зарегистрированных как администраторы IBM Spectrum Protect. Решением IBM Spectrum Protect может управлять один администратор, или обязанности администратора могут быть распределены между несколькими людьми.

Для работы с решением необходимо хорошо знать операционную систему сервера и протоколы связи для среды клиента или сервера. Также необходимо понимать принципы управления хранением данных в вашей организации, например, принципы резервного копирования файлов рабочей станции и использования устройств хранения.

Публикации

В семейство продуктов IBM Spectrum Protect входят IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases и ряд других продуктов по управлению хранением от IBM®.

Документацию к продуктам IBM смотрите на веб-странице IBM Knowledge Center.

Что нового в этом выпуске

Этот выпуск IBM Spectrum Protect содержит новые функции и обновления.

Список новых функций и обновлений смотрите в разделе Что нового.

Новая и измененная информация в этой документации по продукту отмечена вертикальной чертой (|) слева от изменения.

Часть 1. 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.

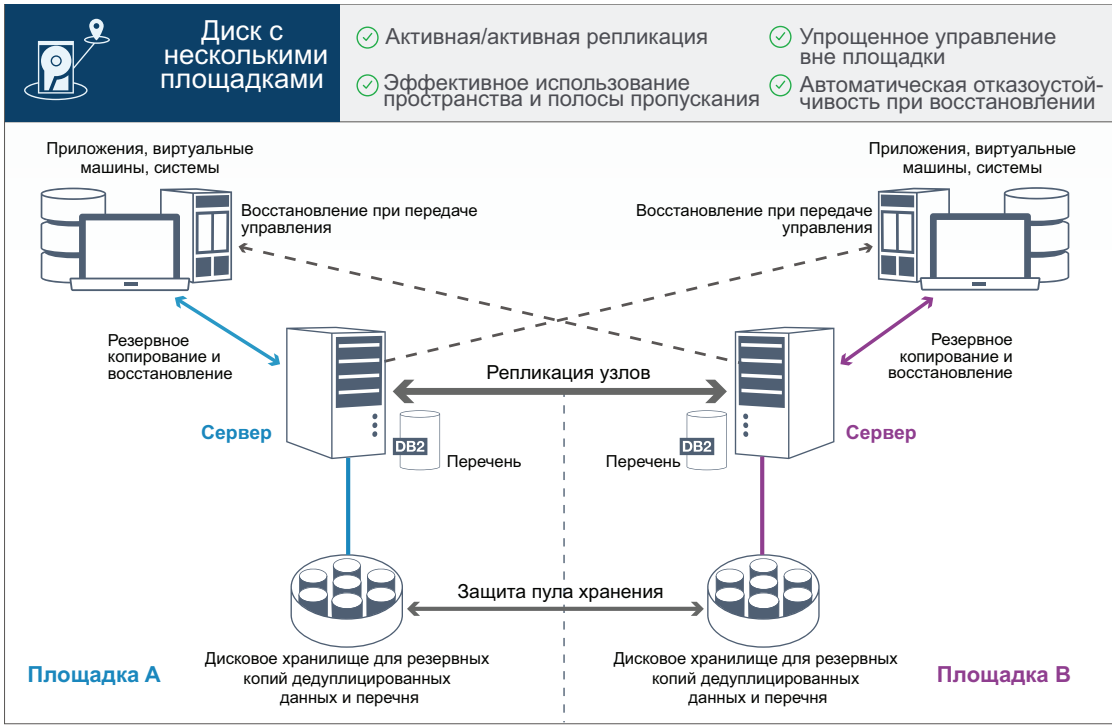


Рисунок 1. Решение с несколькими площадками

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.

Глава 1. 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.

Таблица 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.

Глава 2. 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:

Глава 3, “Требования к системе для дискового решения с несколькими площадками”, на стр. 9

Глава 3. 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.

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 Глава 1, “Выбор размера системы”, на стр. 3.

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	AIX 6 ядер процессора, 3,42 ГГц или быстрее Linux Windows 16 ядер процессора, 1,7 ГГц или быстрее	AIX 10 ядер процессора, 3,42 ГГц или быстрее Linux Windows 20 ядер процессора, 2,2 ГГц или быстрее	AIX 20 ядер процессора, 3,42 ГГц Linux 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)

Аппаратный компонент	Небольшая система	Средняя система	Крупная система
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 .

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

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

Задачи, связанные с данной:

Настройка сетевых опций AIX

Глава 4. 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

Таблица 2. 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. 3 на стр. 18.
Каталог для установки сервера	/		Доступное пространство, необходимое для каталога: 5 ГБ	

Таблица 2. Рабочая таблица для предварительного конфигурирования серверной системы AIX (продолжение)

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
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	

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

Таблица 2. Рабочая таблица для предварительного конфигурирования серверной системы AIX (продолжение)

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

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.

Таблица 3. 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. 2 на стр. 15, 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`		
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.

Таблица 3. Рабочая таблица для конфигурирования IBM Spectrum Protect (продолжение)

Элемент	Значение по умолчанию	Собственное значение	Примечания
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

Таблица 4. Рабочая таблица для предварительного конфигурирования серверной системы Linux

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. 5 на стр. 21.
Каталог для активного журнала	/tsminst1/TSMalog		• Небольшие и средние: 140 ГБ • Крупные: 300 ГБ	

Таблица 4. Рабочая таблица для предварительного конфигурирования серверной системы Linux (продолжение)

Элемент	Значение по умолчанию	Собственное значение	Минимальный размер каталога	Примечания
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

Таблица 4. Рабочая таблица для предварительного конфигурирования серверной системы Linux (продолжение)

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.

Таблица 5. 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. 4 на стр. 19, 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`		

Таблица 5. Рабочая таблица для конфигурирования IBM Spectrum Protect (продолжение)

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.

Таблица 6. Рабочая таблица для предварительного конфигурирования серверной системы Windows

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. 7 на стр. 25.
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

Таблица 6. Рабочая таблица для предварительного конфигурирования серверной системы Windows (продолжение)

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

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.

Таблица 7. 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. 6 на стр. 23, 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.		
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.

Таблица 7. Рабочая таблица для конфигурирования IBM Spectrum Protect (продолжение)

Элемент	Значение по умолчанию	Собственное значение	Примечания
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.

Глава 5. 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

Ссылки, связанные с данной:

Требования к системе хранения и уменьшение риска повреждения данных

Планирование массивов хранения

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

Вы разрабатываете массивы хранения, размер и характеристики производительности которых подходят для одного из компонентов серверного хранилища IBM Spectrum Protect, например, базы данных сервера или пула хранения. Операция планирования хранения должна учитывать тип накопителя, уровень RAID, число накопителей, число запасных накопителей и т.п. В конфигурациях решения группы хранения содержат массивы RAID внутреннего хранения, которые состоят из нескольких физических дисков, представленных в системе в виде логических томов. При конфигурировании дисковой системы хранения вы создаете группы хранения или пулы хранения данных, а затем создаете массивы хранения в группах.

Вы создаете тома или LUN из групп хранения. Группа хранения задает, какие диски обеспечивают пространство хранения, составляющее том. При создании томов сделайте их полностью выделенными. Используются более быстрые типы дисков, чтобы хранить тома базы данных и активные тома журнала. Более медленные типы

дисков можно использовать для томов пула хранения, архивного журнала и томов резервных копий базы данных. Если для подготовки данных используется меньший пул хранения на основе дисков, вам, возможно, придется использовать более быстрые диски, чтобы справиться с ежедневной рабочей нагрузкой по поглощению и перенастройке данных.

В разделах Табл. 8 и Табл. 9 описаны требования к схеме для конфигурации групп хранения и томов.

Таблица 8. Компоненты конфигурации группы хранения

Компонент	**Подробности**
Требования к пространству хранения на сервере	Как сервер использует пространство хранения.
Тип диска	Размер и скорость для типа диска, используемого в соответствии с требованиями хранения.
Количество дисков	Число дисков каждого типа, которые необходимы в соответствии с требованиями к хранению.
Емкость горячего резервирования	Число дисков, зарезервированных в качестве запасных для передачи управления в случае отказа диска.
Уровень RAID	Уровень массива RAID, используемый для логического хранения. Уровень RAID определяет тип избыточности, обеспечиваемой массивом, например 5 или 6.
Количество массивов RAID	Количество создающихся массивов RAID.
DDM на массив RAID	Сколько модулей дисководов (disk drive module, DDM) нужно использовать в каждом из массивов RAID.
Используемый размер на массив RAID	Размер пространства, доступный для хранения данных в каждом массиве RAID после вычета пространства, потерянного вследствие избыточности.
Общий используемый размер	Общий размер, доступный для хранения данных в массивах RAID: `Количество x Используемый размер`
Рекомендуемые имена групп хранения и массивов	Предпочтительное имя, которе следует использовать для дисков MDisk и групп MDisk.
Использование	Компонент сервера, который использует часть физического диска.

Таблица 9. Компоненты конфигурации томов

Компонент	**Подробности**
Требования к пространству хранения на сервере	Требования, в соответствии с которыми используется физический диск.
Имя тома	Уникальное имя, присвоенное отдельному тому.
Группа хранения	Имя группы хранения, для которой будет взято пространство, чтобы создать том.
Размер	Размер каждого тома.
Предполагаемая точка монтирования сервера	Каталог на компьютере сервера, где монтируется том.

Таблица 9. Компоненты конфигурации томов (продолжение)

Компонент	Подробности
Количество	Число томов, которые нужно создать для выполнения определенных требований. Используйте один и тот же стандарт присвоения имен для каждого тома, созданного в соответствии с теми же требованиями.
Использование	Компонент сервера, который использует часть физического диска.

Примеры

Примеры конфигурации для групп хранения и томов можно найти, воспользовавшись следующей ссылкой: Примеры рабочих листов для планирования массивов хранения. В примерах показано, как спланировать хранение при разных размерах серверов. В конфигурациях примеров существует отображение один на один между дисками MDisk и группами storage. Можно скачать примеры и изменить рабочие листы, чтобы спланировать конфигурацию хранения для сервера.

Глава 6. 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.

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. 10 представлены примеры того, почему вам может потребоваться назначить разные уровни полномочий, чтобы администраторы могли выполнять задачи:

Таблица 10. 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

Таблица 10. Сценарии для ролей администраторов (продолжение)

Сценарий	Тип ID администратора, который нужно задать
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. 11 описаны порты, используемые сервером, клиентом и компонентом Центр операций.

Таблица 11. 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.

Таблица 11. Порты, используемые сервером, клиентом и компонентом Центр операций (продолжение)

Элемент	По умолчанию	Направление	Описание
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**.
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.

Таблица 11. Порты, используемые сервером, клиентом и компонентом Центр операций (продолжение)

Элемент	По умолчанию	Направление	Описание
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.

Часть 2. 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.

Глава 7. 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.

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 Глава 5, “Планирование хранения”, на стр. 27.
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.

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. 12. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Таблица 12. 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. 13, 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 к IBM Db2 версии 11.1.

Таблица 13. 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. Разрешает ASLR для серверов V7.1 и новее. 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. 14. Если значения ulimit заданы неправильно, вы можете столкнуться с нестабильностью сервера или ошибкой ответа сервера.

Таблица 14. 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

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
    33213600507630081010578000000000000030042145O3IBMfcp
   ```

   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.
   - AIX Linux Создайте 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:

     AIX

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

     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.

   - Windows Создайте 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.

Системы 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” на стр. 50, есть права доступа для чтения и записи к каталогам на сервере IBM Spectrum Protect.

Системы 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” на стр. 50, есть права доступа для чтения и записи к каталогам для IBM Spectrum Protect.

Системы 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.

Глава 8. 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.

Прежде чем начать

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

Процедура

1. AIX Убедитесь, что у вас в системе установлены необходимые файлы RPM.

   Дополнительные сведения смотрите в разделе “Установка обязательных файлов RPM для графического мастера” на стр. 56.
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. AIX Убедитесь, 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.

Задачи, связанные с данной:

Другие методы установки компонентов IBM Spectrum Protect (AIX)

Другие методы установки компонентов IBM Spectrum Protect (Linux)

Установка обязательных файлов RPM для графического мастера

AIX

Файлы RPM необходимы для графического мастера IBM Installation Manager.

Процедура

1. Убедитесь, что у вас в системе установлены следующие файлы: Если файлы не установлены, перейдите к шагу 2.

```
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
```

2. Убедитесь, что в файловой системе `/opt` свободно, по крайней мере, 150 МБ пространства.
3. В каталоге, в который извлечен файл пакета установки, перейдите в подкаталог `gtk`.
4. Скачайте файлы RPM в текущий рабочий каталог с веб-сайта IBM AIX Toolbox for Linux Applications, введя следующую команду:

```
download-prerequisites.sh
```

5. Установите скачанные файлы RPM в каталоге, в котором они находятся, введя следующую команду:

```
rpm -Uvh *.rpm
```

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

Глава 9. 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.

Прежде чем начать

Убедитесь, что выполнены следующие требования:

AIX 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.

Windows Убедитесь, 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.
   - AIX Linux Откройте программу `dsmicfgx` в каталоге `/opt/tivoli/tsm/server/bin`. Этот мастер можно запустить только от имени пользователя root.
   - Windows Щелкните по **Пуск > Все программы > IBM Spectrum Protect > Мастер конфигурирования**.
2. Завершите конфигурирование, следуя инструкциям. Используйте информацию, записанную вами в таблицу Глава 4, “Рабочие листы планирования”, на стр. 15 в ходе настройки системы IBM Spectrum Protect, чтобы задать каталоги и опции в мастере.

   AIX Linux В окне Информация о сервере задайте автоматический запуск сервера при загрузке системы, используя ID пользователя экземпляра.

   Windows При 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)

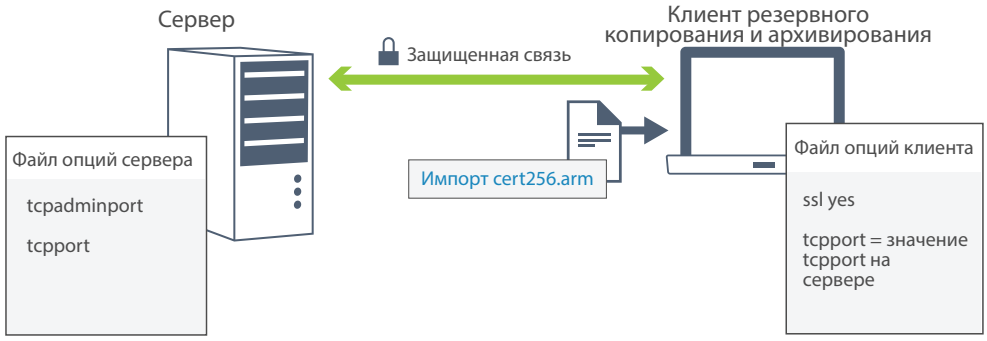
Конфигурирование защищенной связи с использованием Transport Layer Security (TLS)

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 Глава 16, “Состояние системы отслеживания с использованием отчетов по электронной почте”, на стр. 105.

Защита связи между компонентом Центр операций и хаб-сервером

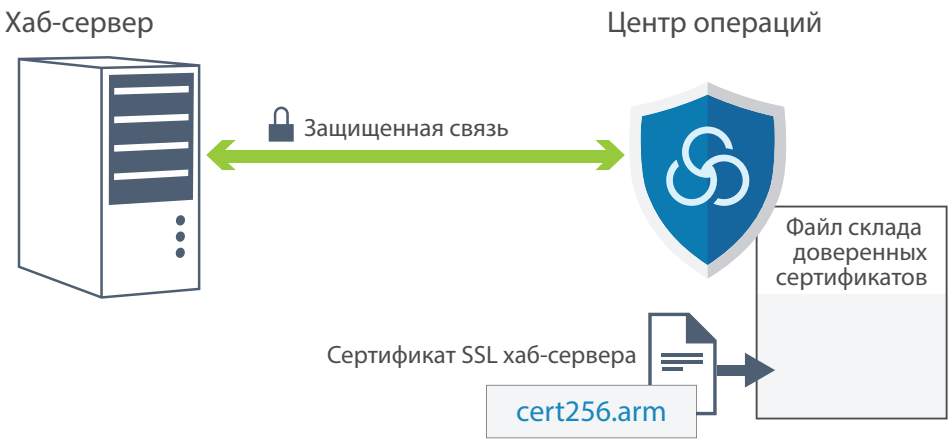
Для защиты связи между компонентом Центр операций и хаб-сервером добавьте сертификат Transport Layer Security (TLS) хаб-сервера в файл доверенного хранилища компонента Центр операций.

Прежде чем начать

Файл доверенного хранилища компонента Центр операций - это контейнер сертификатов, доступ к которому может получить Центр операций. Он содержит сертификат, который Центр операций использует для связи HTTPS с веб-браузерами.

При установке компонента Центр операций вы создаете пароль для файла склада доверенных сертификатов. 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.

На следующем рисунке показаны компоненты для настройки SSL между компонентом Центр операций и хаб-сервером.



Об этой задаче

В этой процедуре описаны шаги по реализации защищенной связи с использованием самоподписанных сертификатов.

Процедура

Чтобы настроить связь SSL с использованием самоподписанных сертификатов, сделайте следующее:

1. Задайте сертификат `cert256.arm` в качестве сертификата по умолчанию в файле базы данных ключей хаб-сервера:
   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.
   c. Убедитесь, что сертификат `cert256.arm` задан как сертификат по умолчанию. Введите следующую команду:
      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
2. Остановите веб-сервер Центр операций.
3. Откройте командную строку операционной системы в системе, где установлен компонент Центр операций, и перейдите в следующий каталог:
   - AIX Linux *каталог_установки*`/ui/jre/bin`
   - Windows *каталог_установки*`\ui\jre\bin`

   Где *каталог_установки* - это каталог, в котором установлен компонент Центр операций.
4. Откройте окно Управление ключами IBM, введя следующую команду:

ikeyman

5. Выберите **Файл базы данных ключей > Открыть**.
6. Щелкните по **Обзор** и перейдите в следующий каталог, где *каталог_установки* - это каталог, в котором установлен компонент Центр операций:
   - AIX Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Windows *каталог_установки*\ui\Liberty\usr\servers\guiServer
7. Выберите в каталоге guiServer файл gui-truststore.jks.
8. Щелкните по **Открыть**, а затем по **OK**.
9. Введите пароль для файла доверенного хранилища и щелкните по **OK**.
10. В области Контент базы данных ключей окна Управление ключами IBM щелкните по стрелке и выберите в списке **Сертификаты подписывающих**. Щелкните по **Добавить**.
11. В окне Открыть щелкните по **Обзор** и перейдите в каталог экземпляра хаб-сервера:
    - AIX Linux /opt/tivoli/tsm/server/bin
    - Windows c:\Program Files\Tivoli\TSM\server1

    В каталоге содержится сертификат cert256.arm.

    Если из окна Открыть недоступен каталог экземпляра хаб-сервера, выполните следующие действия:

    a. При помощи FTP или другого способа передачи файлов скопируйте файлы cert256.arm с хаб-сервера в следующий каталог на компьютере, на котором установлен компонент Центр операций:
       - AIX Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
       - Windows *каталог_установки*\ui\Liberty\usr\servers\guiServer

    b. В окне Открыть перейдите в каталогguiServer.
12. Выберите сертификат cert256.arm в качестве сертификата SSL.
13. Щелкните по **Открыть**, а затем по **OK**.
14. Введите метку для сертификата. Например, задайте имя хаб-сервера.
15. 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.
16. Закройте окно Управление ключами IBM.
17. Запустите веб-сервер Центра операций. 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.

Задачи, связанные с данной:

“Запуск и остановка веб-сервера” на стр. 111

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.
- Linux Вы 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 Глава 4, “Рабочие листы планирования”, на стр. 15.

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” на стр. 118

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.
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.

   AIX Linux Например, 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"
   ```

   Windows Например, 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
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” на стр. 67.

Глава 10. 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.

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:
  1. В панели меню Центра операций выберите **Клиенты**.
  2. В таблице Клиенты щелкните по **+ Клиент**.
  3. Выполните шаги в мастере Добавить клиент:

a. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель **Включить** в области Дедупликация данных на стороне клиента.

b. 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.

c. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.

d. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.

e. 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.

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.

Глава 11. 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. Глава 7, “Настройка системы”, на стр. 39
   b. Глава 8, “Установка сервера и компонента Центр операций”, на стр. 55

      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. Глава 9, “Конфигурирование сервера и компонента Центр операций”, на стр. 59

      Пропустите задачи по конфигурированию компонента Центр операций.
   d. Глава 10, “Установка и конфигурирование клиентов резервного копирования и архивирования”, на стр. 71
2. “Конфигурирование связи SSL между хаб-сервером и подчиненным сервером”
3. “Добавление второго сервера как подчиненного сервера” на стр. 79
4. “Как включить репликацию” на стр. 79

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” на стр. 67.
   - 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.

Глава 12. 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 Часть 3, “Мониторинг дискового решения с несколькими площадками”, на стр. 83.

Часть 3. 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” на стр. 72.

Процедура

1. Выполните задачи ежедневного мониторинга. Инструкции смотрите в разделе Глава 13, “Контрольный список ежедневного мониторинга”, на стр. 85.
2. Выполните задачи периодического мониторинга. Инструкции смотрите в разделе Глава 14, “Контрольный список периодического мониторинга”, на стр. 95.
3. Чтобы проверить, соответствует ли ваше решение IBM Spectrum Protect требованиям по лицензированию, следуйте инструкциям в разделе Глава 15, “Проверка на соответствие лицензии”, на стр. 103.
4. Как сконфигурировать центр операций для генерирования отчетов о состоянии электронной почты, смотрите в разделе Глава 16, “Состояние системы отслеживания с использованием отчетов по электронной почте”, на стр. 105

Дальнейшие действия

Устраните все обнаруженные вами проблемы. Чтобы устранить проблему, изменив конфигурацию вашего решения, следуйте инструкциям в разделе Часть 4, “Управление операциями для дискового решения с несколькими площадками”, на стр. 107. Кроме того, существуют следующие ресурсы:

- Информацию об устранении проблем производительности смотрите в разделе Производительность.

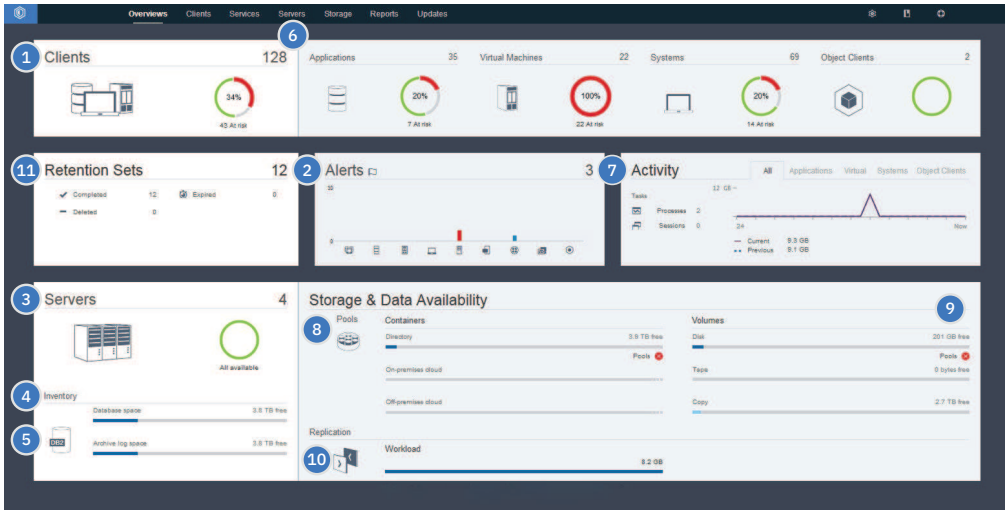
- Информацию об устранении других проблем смотрите в разделе Устранение неполадок.

Глава 13. 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.

Таблица 15. 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:** Уведомления доступны только для клиентов резервного копирования и архивирования и для клиентов IBM Spectrum Protect for Virtual Environments. • 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.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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**.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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 вкладку **Приложения**, **Виртуальные машины** или **Системы**. • Если на сервер было отправлено меньше данных, чем вы ожидали, выясните, выполняются ли операции резервного копирования клиентов по расписанию.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
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-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.	Чтобы увидеть емкость пула хранения, используемую за последние две недели, выберите строку в таблице Пулы хранения данных и щелкните по **Сведения**.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

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 назначения репликации, выполните следующие шаги: 1. Щелкните на странице Обзор в компоненте Центр операций по **Серверы**. 2. Выберите исходный сервер репликации или сервер назначения репликации 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.

Таблица 15. Задачи ежедневного мониторинга (продолжение)

Задача	Основные процедуры	Дополнительные процедуры и диагностическая информация
11 Мониторинг наборов хранения.	Чтобы получить общее состояние наборов хранения, просмотрите область **Наборы хранения** на странице Центр операцийОбзор: • В поле **Выполнено** указано число наборов хранения, созданных в базе данных сервера и отслеживаемых в перечне сервера. • В поле **Срок действия истек** указывается число наборов хранения, для которых истек срок хранения данных. • В поле **Удалено** указывается число наборов хранения, которые были удалены. Чтобы просмотреть или изменить правила хранения, выберите **Службы > Правила хранения**.	Чтобы получить дополнительную информацию о наборах хранения, щелкните по области **Наборы хранения**, чтобы открыть страницу Наборы хранения. Чтобы просмотреть или изменить свойства набора хранения, дважды щелкните по набору хранения. Более подробную информацию можно получить, выполнив связанные команды: 1. На странице Обзор компонента Центр операций установите указатель мыши на значок параметров и щелкните по **Построитель команд**. 2. Чтобы узнать, какие задания создания набора хранения выполняются, прерваны или завершены, выполните команду **QUERY JOB**. Инструкции смотрите в разделе QUERY JOB (Запросить задание создания набора хранения). 3. Чтобы запросить правила хранения, введите команду **QUERY RETRULE**. Инструкции смотрите в разделе QUERY RETRULE (запрос правила хранения). 4. Чтобы запросить наборы хранения, введите команду **QUERY RETSET**. Инструкции смотрите в разделе QUERY RETSET (запрос набора хранения). 5. Чтобы запросить содержимое набора хранения, введите команду **QUERY RETSETCONTENTS**. Инструкции смотрите в разделе QUERY RETSETCONTENTS (запрос содержимого набора хранения).

Глава 14. 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**.

Таблица 16. 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.

Таблица 16. Задачи периодического мониторинга (продолжение)

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.	

Таблица 16. Задачи периодического мониторинга (продолжение)

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: • 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. • 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. • 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: • AIX Linux `/home/tsminst1/tsminst1` • Windows `C:\tsminst1` **Совет:** Если вы заполнили рабочую таблицу планирования, расположение каталога экземпляров записано в рабочей таблице.	

Таблица 16. Задачи периодического мониторинга (продолжение)

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

Таблица 16. Задачи периодического мониторинга (продолжение)

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.

Таблица 16. Задачи периодического мониторинга (продолжение)

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)

Глава 15. 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. IBM License Metric Tool предназначен для отслеживания фактического использования. Например, после установки Клиент резервного копирования и архивирования IBM Spectrum Protect этот инструмент учитывает клиента только после первого использования.

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	1. В строке меню компонента Центр операций установите указатель мыши на значок параметров  и щелкните по **Лицензирование**. На странице Фронтальное использование показана оценка фронтальной емкости. 2. Если в столбце Нет отчета показано значение, щелкните по числу, чтобы узнать о клиентах, которые не сообщили об использовании емкости. 3. 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. 4. Прибавьте оценку для компонента Центр операций и все оценки, которые вы получили с использованием сценария. 5. 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. 1. В строке меню компонента Центр операций установите указатель мыши на значок параметров  и щелкните по **Лицензирование**. 2. Щелкните по вкладке **Внутренний**. 3. 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.

Глава 16. 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)

Часть 4. 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.

Глава 17. 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*.

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 Центра 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.
   - AIX В каталоге */каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:
     ```
     ./stopserver.sh
     ```
   - Linux Введите следующую команду:
     ```
     service opscenter.rc stop
     ```
   - Windows В окне Службы остановите службу **Центр операций IBM Spectrum Protect**.
2. Запустите веб-сервер.
   - AIX В каталоге */каталог_установки*/ui/utils, где *каталог_установки* - это каталог установленного Центр операций, введите следующую команду:
     ```
     ./startserver.sh
     ```
   - Linux Введите следующие команды:

     Запустите сервер:
     ```
     service opscenter.rc start
     ```

     Перезапустите сервер:
     ```
     service opscenter.rc restart
     ```

     Определите, работает ли сервер:
     ```
     service opscenter.rc status
     ```
   - Windows В 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:
   - AIX Linux *каталог_установки*/ui/Liberty/usr/servers/guiServer
   - Windows *каталог_установки*\ui\Liberty\usr\servers\guiServer

   Например:
   - AIX Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows c:\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” на стр. 111

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” на стр. 111

“Запуск и остановка веб-сервера” на стр. 111

Глава 18. 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.

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” на стр. 116.
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” на стр. 118.
3. Укажите, когда следует производить резервное копирование и архивирование клиентских данных. Следуйте инструкциям в разделе “Планирование операций резервного копирования и архивирования” на стр. 121.

4. Чтобы позволить клиенту соединяться с сервером, зарегистрируйте клиент. Следуйте инструкциям в разделе “Регистрация клиентов” на стр. 122.
5. Чтобы начать защищать клиентский узел, установите и сконфигурируйте выбранную программу на клиентском узле. Следуйте инструкциям в разделе “Установка и настройка клиентов” на стр. 123.

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” на стр. 123.

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

Цель	Продукт и описание	Инструкции по установке
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 Db2	API (application programming interface, интерфейс прикладного программирования) клиента резервного копирования и архивирования 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 Data Protection for SAP for Db2 • Установка Data Protection for SAP for Oracle
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” на стр. 121.
- 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” на стр. 119.
2. Если необходимо внести незначительные изменения для соответствия требованиям хранения данных, следуйте инструкциям в разделе “Изменение политик” на стр. 119.

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	1. В таблице Наборы политик щелкните по **+Класс управления**. 2. Чтобы задать правила для резервного копирования и архивирования данных, заполните поля в окне Добавить класс управления. 3. Чтобы сделать класс управления классом управления по умолчанию, включите переключатель **Сделать значением по умолчанию**. 4. 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” на стр. 122.
- 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	1. В представлении Расписания выберите расписание и щелкните по **Сведения**. 2. На странице Сведения о расписании просмотрите сведения, щелкнув по синим стрелкам в начале строк. 3. 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 (Задать запланированное задание клиента) 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:
  1. В панели меню Центра операций выберите **Клиенты**.
  2. В таблице Клиенты щелкните по **+ Клиент**.
  3. Выполните шаги в мастере Добавить клиент:
     a. Укажите, что избыточные данные можно устранить как на клиенте, так и на сервере. Выберите переключатель **Включить** в области Дедупликация данных на стороне клиента.
     b. 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.
     c. Следуйте инструкциям в мастере, чтобы задать домен политики, расписание и набор опций.
     d. Укажите, как для клиента будут показаны риски, задав параметр Под угрозой.
     e. 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 на стр. 124.

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 клиентов.
IBM Spectrum Protect for Databases	• Установка Data Protection for Oracle • Установка Data Protection for SQL Server в ядре сервера Windows

Программа	Ссылка на инструкции
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 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 Data Protection for SAP for Db2 • Установка 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.	• 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” на стр. 122).
   - 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” на стр. 72.

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” на стр. 128.
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” на стр. 132.

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

1. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
2. Щелкните по вкладке **Веб-клиент**.
3. 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**.
4. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции **passwordaccess** в файле `dsm.sys` значение `generate`.
5. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

   ```
   dsmc query sess
   ```
6. Запустите приемник клиента, введя в командной строке следующую команду:

   ```
   /usr/bin/dsmcad
   ```
7. 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

1. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
2. Щелкните по вкладке **Веб-клиент**.
3. 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**.
4. Чтобы убедиться, что планировщик может запуститься без участия оператора, задайте для опции **passwordaccess** в файле `dsm.sys` значение `generate`.
5. Чтобы сохранить пароль клиентского узла, введите следующую команду и укажите пароль клиентского узла, когда вам это предложат:

   ```
   dsmc query sess
   ```
6. Запустите приемник клиента, войдя в систему от имени ID пользователя root и введя следующую команду:

   ```
   service dsmcad start
   ```
7. Чтобы включить автоматический запуск приемника клиента после перезапуска системы, добавьте службу, введя в командной строке оболочки следующую команду:

   ```
   # chkconfig --add dsmcad
   ```

MAC OS X

1. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Изменить > Предпочтения клиента**.
2. Чтобы планировщик мог запускаться без участия оператора, щелкните по **Авторизация**, выберите **Генерирование пароля**и щелкните по **Применить**.
3. Чтобы указать, как осуществляется управление службами, щелкните по **Веб-клиент**, выберите **Расписание**, щелкните по **Применить** и выберите **OK**.
4. Чтобы сгенерированный пароль был сохранен, перезапустите клиент резервного копирования и архивирования.
5. Используйте для запуска приемника клиента приложение Инструменты IBM Spectrum Protect для администраторов.

Windows

1. В графическом пользовательском интерфейсе клиента резервного копирования и архивирования выберите **Утилиты > Мастер настройки > Помочь мне сконфигурировать Планировщик клиента**. Щелкните по **Далее**.
2. Прочтите информации на странице мастера планировщика и нажмите **Далее**.
3. На странице Задача планировщика выберите **Установить новый или дополнительный планировщик** и нажмите **Далее**.
4. 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**.
5. Введите имя, которое вы хотите присвоить этому приемнику клиента. Имя по умолчанию - Client Acceptor. Щелкните по **Далее**.
6. Выполните конфигурирование, выполняя шаги в мастере.
7. Обновите файл опций клиента, `dsm.opt`, и задайте для опции **`passwordaccess`** значение `generate`.
8. Чтобы сохранить пароль клиентского узла, введите в командной строке следующую команду:

   ```
   dsmc query sess
   ```

   Когда вам это предложат, введите пароль клиентского узла.
9. 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.

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” на стр. 72. Инструкции по проверке установки смотрите в разделе “Проверка того, правильно ли установлена служба управления клиентами” на стр. 73.

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:
  1. 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
     ```
  2. 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:
  1. Выберите **Пуск > Администрирование > Службы**.
  2. Дважды щелкните по службе приемника клиента.
  3. Щелкните по **Остановить** и **OK**.
- Чтобы перезапустить службу приемника клиента, выполните следующие действия:
  1. Выберите **Пуск > Администрирование > Службы**.
  2. Дважды щелкните по службе приемника клиента.
  3. 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 клиентов
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

Программа	Ссылка на инструкции
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.

Ограничение: Нельзя списать клиентский узел объектов.

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)

Глава 19. Управление хранилищем данных

Управляйте данными эффективно и добавьте на сервер поддерживаемые устройства и носители, чтобы хранить данные клиента.

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 IBM 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:

Таблица 17. 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 Часть 3, “Мониторинг дискового решения с несколькими площадками”, на стр. 83.
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.

Понятия, связанные с данным:

Производительность

Задачи, связанные с данной:

Дедупликация данных (V7.1.1)

“Как задать расписания для операций по обслуживанию сервера” на стр. 67

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.

Прежде чем начать

Спланируйте емкость вашего решения, чтобы у вас на сервере было достаточно пространства для клиентских узлов, включая пространство для роста в будущем.

Об этой задаче

При перемещении клиентских узлов можно оставить их существующие резервные копии на исходном сервере, чтобы срок их действия истек в соответствии с вашей политикой устаревания, или можно экспортировать их существующие резервные копии на новый сервер.

Процедура

Чтобы переместить узел клиента на другой сервер, выполните следующие шаги:

1. Экспортируйте клиентский узел непосредственно на новый сервер при помощи команды **EXPORT NODE**.
2. Обновите файл опций клиента, используя новое имя сервера.
3. На новом сервере назначьте расписание для клиентского узла, чтобы произвести резервное копирование данных.
   a. На странице **Клиенты** в компоненте Центр операций выберите клиентский узел.
   b. Выберите **Еще > Связь с расписанием**.
   c. Выберите переключатель в строках расписания, для которого вы хотите назначить выбранные клиентские узлы.
   d. Щелкните по **Сохранить**.
4. Снова введите команду **EXPORT NODE**, чтобы инкрементно экспортировать данные с исходного сервера на новый сервер. Выполняя инкрементный экспорт данных, вы экспортируете данные, резервная копия которых была создана в промежутке между первым процессом экспорта и моментом, когда когда вы назначили расписание для клиентского узла.
5. Произведите мониторинг клиентского узла, чтобы убедиться, что резервное копирование данных производится в соответствии с заданным вами расписанием, и чтобы проверить, не находится ли клиентский узел под угрозой. Установите указатель мыши на **Клиенты** и щелкните по **Расписания**.
6. Спишите клиентский узел с исходного сервера, выполнив следующие шаги:
   a. На странице **Обзор** в компоненте Центр операций щелкните по **Клиенты**.
   b. Выберите клиентский узел в таблице Клиенты.
   c. Выберите **Еще > Списать**.

   Клиентский узел будет удален с исходного сервера. Когда закончится срок хранения данных, указанный в параметрах политики, данные клиентского узла будут удалены. После удаления данных клиентского узла клиент удаляется с сервера.

Ссылки, связанные с данной:

EXPORT NODE (экспорт данных клиентского узла)

 IMPORT NODE (импорт данных клиентского узла)

Глава 20. 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 назначения репликации совместимы для репликации.

Таблица 18. Совместимость репликации для разных версий серверов

Версия сервера репликации источника	Совместимые версии для сервера назначения репликации
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
V8.1.6	V7.1.3 или новее
V8.1.7	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:

1. Щелкните на странице Серверы по **Сведения**.
2. На странице Сведения щелкните по **Свойства**.
3. В разделе **Репликация** выберите **Включена** в поле **Исходящая репликация**.
4. Щелкните по **Сохранить**.

Дальнейшие действия

Выполните следующие действия:

1. Чтобы узнать, успешно ли выполнена репликация, смотрите раздел Глава 13, “Контрольный список ежедневного мониторинга”, на стр. 85.
2. Linux Если 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” на стр. 147

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 Глава 13, “Контрольный список ежедневного мониторинга”, на стр. 85.
2. Linux Если 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.	1. Щелкните на странице Серверы по **Сведения**. 2. На странице Сведения щелкните по **Свойства**. 3. 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**. 4. Щелкните по **Сохранить**.

Задача	Процедура
Укажите, в течение какого времени сохраняются записи репликации.	1. Щелкните на странице Серверы по **Сведения**. 2. На странице Сведения щелкните по **Свойства**. 3. 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. 4. Щелкните по **Сохранить**.
Задайте целевой сервер репликации.	1. Щелкните на странице Серверы по **Сведения**. 2. На странице Сведения щелкните по **Свойства**. 3. В разделе **Репликация** задайте целевой сервер. 4. Щелкните по **Сохранить**.
Отмените процесс репликации.	1. Щелкните на странице Серверы по **Активные задачи**. 2. Выберите процесс или сеанс, который вы хотите отменить. 3. 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” на стр. 119.
   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 назначения репликации, 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 назначения репликации CVT_SRV2, введите на исходном сервере следующую команду:

```
set dissimilarpolicies cvt_srv2 on
```

В следующий раз, когда запустится процесс репликации, политики на сервере назначения репликации 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 назначения репликации не совпадают, будет использоваться политика, заданная для исходного сервера репликации. Если вы включите политику на сервере назначения репликации, используя команду **SET DISSIMILARPOLICIES**, будет использоваться политика, заданная для сервера назначения репликации. Если на сервере назначения репликации 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 назначения репликации, чтобы управлять реплицированными данными)

VALIDATE REPLICATION (Проверить репликацию для клиентского узла)

VALIDATE REPLPOLICY (Проверить политики на сервере назначения репликации)

Глава 21. 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.

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 IBM 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).

Таблица 19. 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.

  Примечание: 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.

Таблица 20. 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 успешно аутентифицируется на сервере с использованием программного обеспечения V8.1.2 или более новой версии, или V7.1.8 или более новой версии, администратор больше не сможет пройти аутентификацию на этом сервере, используя версии клиента или сервера более ранней версии, чем V8.1.2 или V7.1.8. 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 **SELECT**Ю 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:
	1. Зарегистрируйте администратора и задайте **Pa$#$twO** в качестве пароля, введя следующую команду:
	`register admin admin1 Pa$#$twO`
	2. 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`

Задача	Процедура
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.

Таблица 21. Задачи по аутентификации для серверов IBM Spectrum Protect

Задача	Процедура
Задать максимальное число попыток ввода неправильного пароля.	1. Выберите сервер на странице Серверы Центра операций. 2. Щелкните по **Сведения**, а затем по вкладке **Свойства**. 3. Задайте число неудачных попыток в поле **Предел неудачных попыток входа в систему**. Значение по умолчанию при установке равно 0.
Задайте минимальную длину пароля.	1. Выберите сервер на странице Серверы Центра операций. 2. Щелкните по **Сведения**, а затем по вкладке **Свойства**. 3. Задайте число символов в поле **Минимальная длина пароля**.
Задайте срок действия паролей.	1. Выберите сервер на странице Серверы Центра операций. 2. Щелкните по **Сведения**, а затем по вкладке **Свойства**. 3. Задайте срок в днях в поле **Общий срок действия паролей**.

Таблица 21. Задачи по аутентификации для серверов IBM Spectrum Protect (продолжение)

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.

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” на стр. 156.

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. 22).

Таблица 22. 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.

Таблица 22. Опции сервера и доступ к портам (продолжение)

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.

Ссылки, связанные с данной:

“Планирование доступа через брандмауэр” на стр. 33

Глава 22. 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.

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.
   - AIX Запуск экземпляра сервера
   - Linux Запуск экземпляра сервера
   - Windows Запуск экземпляра сервера

Операции, которые были отключены во время режима обслуживания, будут снова включены.

Глава 23. 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:

- AIX Установка пакета исправлений сервера IBM Spectrum Protect
- Linux Установка пакета исправлений сервера IBM Spectrum Protect
- Windows Установка пакета исправлений сервера IBM Spectrum Protect

Информация, связанная с данной:

Процесс обновления и перенастройки - Часто задаваемые вопросы

Глава 24. 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**).

Глава 25. 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.

Об этой задаче

В случае дискового решения с несколькими площадками используйте репликацию узла, чтобы убедиться, что данные доступны на целевом сервере на площадке восстановления и что время восстановления невелико. В случае сбоя исходный сервер сможет автоматически передать управление серверу назначения для восстановления данных. Если произойдет авария и исходный сервер окажется недоступен, клиентские узлы смогут автоматически записать информацию о целевом сервере репликации в файле опций клиента. Возможно, вам придется вручную обновить файл опций клиентов для более старых клиентов.

Процедура

1. Чтобы вручную производить восстановление данных с целевого сервера репликации, обновите файл опций клиента, указав целевой сервер репликации. Изменять параметры репликации узлов не нужно.
2. Сконфигурируйте клиентский узел, чтобы сохранить данные на целевом сервере репликации.

   Ограничение: Клиентские узлы, которые обычно производят резервное копирование данных на исходный сервер репликации, не могут создавать резервные копии данных на клиентские узлы, реплицируемые на целевой сервер репликации.
3. Проверьте восстановление данных клиента, выполнив следующие шаги:
   a. Восстановите систему клиента в аналогичную операционную систему. Используйте те же самые имена файловой системы с тем же самым объемом файлового пространства в файловой системе.
   b. Восстановите данные в системе, где достаточно пространства для данных.

c. Убедиться, что клиент успешно восстановлен. Например, если вы восстанавливаете виртуальную машину, убедитесь, что виртуальная машина включается, и проверьте, доступны ли файлы.

Задачи, связанные с данной:

Репликация данных на клиентском узле после восстановления базы данных (V7.1.1)

Глава 20, “Управление репликацией”, на стр. 147

Глава 26. Восстановление после 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**
Пул хранения каталога-контейнера	Чтобы восстановить пулы хранения каталогов-контейнеров, сделайте следующее: 1. Просканируйте поврежденные экстенты данных в пуле хранения каталогов-контейнеров, используя команду **AUDIT CONTAINER** и задав параметр **ACTION=SCANALL**. 2. Исправьте поврежденные экстенты данных в пуле хранения каталогов-контейнеров, используя команду **REPAIR STGPOOL**. **Ограничение:** Пул хранения можно исправить, только если пул хранения защищен. 3. Удалите поврежденные экстенты данных, используя команду **AUDIT CONTAINER** и указав параметр **ACTION=REMOVEDAMAGED**.	“Исправление пулов хранения данных” на стр. 176

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” на стр. 175 • SET FAILOVERHLADDRESS (Задать высокоуровневый адрес переключения после отказа)
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)

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: AIX Linux

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

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:

      AIX Linux

      ```
      [root@source]$ ls -lR
      ```

      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: После операции восстановления базы данных, если в файловой системе существуют контейнеры, на которые нет ссылок из базы данных сервера, команда **QUERY STGPOOL** неправильно показывает использование пула хранения. Когда вы выполняете восстановление базы данных до точки во времени, в файловой системе могут оставаться контейнеры без ссылок на них из базы данных сервера. Чтобы получить точную статистику использования пула хранения, надо вручную удалить контейнеры файловой системы без ссылок на них из базы данных сервера.

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)

Часть 5. Приложения

Приложение. 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:

- Работа с использованием только клавиатуры
- Операции с использованием программы для чтения информации с экрана

Семейство продуктов IBM Spectrum Protect использует новейший стандарт W3C, WAI-ARIA 1.0(www.w3.org/TR/wai-aria/), чтобы обеспечить соответствие разделу US Section 508(www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) и рекомендациям по доступности веб-содержимого (Web Content Accessibility Guidelines (WCAG) 2.0(www.w3.org/TR/WCAG20/). 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 (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

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.

Связанная информация 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 (IBM - Специальные возможности) (www.ibm.com/able).

Замечания

Эта публикация разрабатывалась для продуктов и услуг, предлагаемых в США. Материалы на других языках можно получить в IBM. Однако для доступа к копии продукта или версии продукта вы должны быть владельцем копии или версии.

IBM может не предлагать описанные продукты, услуги и возможности в других странах. Сведения о продуктах и услугах, доступных в настоящее время в вашей стране, можно получить в местном представительстве IBM. Любые ссылки на продукты, программы или услуги IBM не означают явным или неявным образом, что можно использовать только продукты, программы или услуги IBM. Разрешается использовать любые функционально эквивалентные продукты, программы или услуги, если при этом не нарушаются права IBM на интеллектуальную собственность. Однако при этом пользователь сам несет ответственность за оценку и проверку работы с другими (не IBM) продуктами, программами и услугами.

Компания IBM может располагать патентами или рассматриваемыми заявками на патенты, относящимися к предмету данного документа. Получение этого документа не означает предоставления каких-либо лицензий на эти патенты. Запросы относительно лицензий направляйте по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

По поводу лицензий, связанных с использованием наборов двухбайтных символов (DBCS), обращайтесь в отдел интеллектуальной собственности IBM в вашей стране или направьте запрос в письменной форме по адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

КОРПОРАЦИЯ INTERNATIONAL BUSINESS MACHINES ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ОТСУТСТВИЯ НАРУШЕНИЙ, КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ КАКОЙ-ЛИБО КОНКРЕТНОЙ ЦЕЛИ. В некоторых законодательствах для определенных сделок подобные оговорки не допускаются, таким образом, это утверждение может не относиться к вам.

В данной информации могут встретиться технические неточности или типографские опечатки. В публикацию время от времени вносятся изменения, которые будут отражены в следующих изданиях. Фирма IBM может в любое время без уведомления вносить изменения и усовершенствования в продукты и программы, описанные в этой публикации.

Любые ссылки в этой публикации на сайты, не принадлежащие IBM, приведены только для удобства и никоим образом не означают их поддержки. Материалы на этих сайтах не входят в число материалов по данному продукту IBM, и весь риск пользования этими сайтами несете вы сами.

IBM оставляет за собой право на использование и распространение любой предоставленной вами информации любыми способами, какие сочтет приемлемыми, не принимая на себя никаких обязательств перед вами.

Если обладателю лицензии на данную программу понадобятся сведения о возможности: (i) обмена данными между независимо разработанными программами и другими программами (включая данную) и (ii) совместного использования таких данных, он может обратиться по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Такая информация может быть предоставлена при соблюдении определенных положений и условий и, возможно, за определенную плату.

Лицензированная программа, описанная в данном документе, и все лицензированные материалы, доступные с ней, предоставляются IBM на условиях IBM Customer Agreement (Соглашения IBM с заказчиком), Международного соглашения о лицензиях на программы IBM или эквивалентного соглашения.

Показанные здесь данные производительности получены в определенных условиях. Реальные результаты могут быть другими.

Информация о продуктах других компаний (не IBM) получена от поставщиков этих продуктов, из их опубликованных объявлений или из иных общедоступных источников. IBM не производила тестирование этих продуктов и никак не может подтвердить информацию о их точности работы и совместимости, а также прочие заявления относительно продуктов других компаний (не IBM). Вопросы о возможностях продуктов других компаний (не IBM) следует направлять поставщикам этих продуктов.

В этой публикации содержатся примеры данных и отчетов, используемых при выполнении текущих служебных задач. Чтобы проиллюстрировать эти задачи с максимальной наглядностью, в примерах используются имена физических лиц, названия компаний, фирм и продуктов. Все эти имена и названия вымышлены, и любое их сходство с реальными именами и адресами полностью случайно.

ЛИЦЕНЗИЯ НА ПРАВО КОПИРОВАНИЯ:

В этом документе содержатся примеры прикладных программ на языках программирования, которые иллюстрируют методы программирования для различных операционных платформ. Вы имеете право копировать, изменять и распространять эти примеры программ в любой форме без уплаты вознаграждения фирме IBM в целях разработки, применения, сбыта или распространения прикладных программ, соответствующих интерфейсу прикладных программ операционной системы, для которой предназначены эти примеры. Эти примеры не были тщательно протестированы при всех возможных условиях. Поэтому IBM не может гарантировать их надежность, пригодность и функционирование. Пробные

программы предоставляются по принципу 'как есть', без какой-либо гарантии. IBM не несет ответственности ни за какой ущерб, возникший в результате использования примеров программ.

Каждая копия программ примеров или программ, созданных на их основе, должна содержать следующее замечание об авторских правах: © (название вашей компании) (год). Части этого кода построены на основе примеров программ IBM Corp. © Copyright IBM Corp. _введите год или годы_.

Товарные знаки

IBM, логотип IBM и ibm.com - товарные знаки или зарегистрированные товарные знаки International Business Machines Corporation, зарегистрированные во многих странах. Прочие названия продуктов и услуг могут быть товарными знаками IBM или других компаний. Текущий список товарных знаков IBM смотрите на веб-странице "Copyright and trademark information" (Информация об авторских правах и товарных знаках) (www.ibm.com/legal/copytrade.shtml).

Adobe - зарегистрированный товарный знак Adobe Systems Incorporated в США и/или в других странах.

Linear Tape-Open, LTO и Ultrium - товарные знаки HP, IBM Corp. и Quantum в США и в других странах.

Intel и Itanium - товарные знаки или зарегистрированные товарные знаки Intel Corporation или ее филиалов в США и/или других странах.

Linux - зарегистрированный товарный знак Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

Microsoft, Windows и Windows NT - товарные знаки Microsoft Corporation в США и/или в других странах.

Java™ и все товарные знаки и логотипы на основе Java - это товарные знаки или зарегистрированные товарные знаки Oracle и/или аффилированных компаний Oracle.

UNIX - зарегистрированный товарный знак The Open Group в США и других странах.

VMware, VMware vCenter Server и VMware vSphere - это зарегистрированные товарные знаки или товарные знаки VMware, Inc. или подразделений VMware, Inc. в США и/или других зонах юрисдикции.

Положения и условия для документации по продукту

Разрешения на использование этих публикаций предоставляются при соблюдении нижеприведенных положений и условий.

Применимость

Указанные условия и положения добавляются ко всем условиям для веб-сайта IBM.

Личное использование

Вы можете воспроизводить эти публикации для своего личного некоммерческого использования при условии, что при этом будут соблюдены все замечания об имущественных правах. Не разрешается распространять, воспроизводить или составлять производные работы на основе данных публикаций или их частей без выраженного согласия IBM.

Коммерческое использование

Вам предоставляется право воспроизводить эти публикации исключительно в пределах своего предприятия при условии, что будут воспроизведены все замечания об авторских правах. За пределами вашего предприятия вам запрещается распространять эти публикации, полностью или по частям, демонстрировать их или создавать из них производные продукты без явного на то согласия от IBM.

Права За исключением прав, явным образом предоставляемых настоящим разрешением, никаких иных разрешений, лицензий и прав, ни явных, ни подразумеваемых, в отношении публикаций и любой содержащейся в них информации, данных, программ или иной интеллектуальной собственности, не предоставляется.

IBM оставляет за собой право отозвать разрешения, предоставленные этим документом, если, по мнению IBM, использование публикаций наносит ущерб IBM или, как это установлено IBM, вышеприведенные инструкции не соблюдаются должным образом.

Вам не разрешается скачивать, экспортировать или повторно экспортировать эту информацию иначе, чем в полном соответствии с правилами и нормативами, включая все законы и правила Соединенных Штатов об экспорте.

IBM НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ КАСАТЕЛЬНО СОДЕРЖИМОГО ЭТИХ ПУБЛИКАЦИЙ. ПУБЛИКАЦИИ ПРЕДСТАВЛЯЮТСЯ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ) ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ РЫНОЧНОЙ ПРИГОДНОСТИ, НЕНАРУШЕНИЯ ПРАВ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.

Замечания о политике конфиденциальности

В программных продуктах IBM, включая программы как решения служб (“Программные предложения”), могут использоваться cookies или другие технологии для сбора информации по использованию продукта, чтобы помочь конечному пользователю в работе, настроить взаимодействия с конечным пользователем или для иных целей. Во многих случаях предложения ПО не собирают информацию, позволяющую идентифицировать личность. Некоторые наши предложения ПО могут помочь вам собрать информацию, позволяющую идентифицировать личность. Если данное предложение ПО использует cookies для сбора информации, позволяющей идентифицировать личность, то ниже будет приведена конкретная информация об использовании cookies в этом предложении.

Настоящее предложение ПО не использует cookies или иные технологии для сбора информации, позволяющей идентифицировать личность.

Если конфигурации, внедренные для этого Предложения относительно программ, обеспечивают вам, как заказчику, возможность собирать информацию, позволяющую идентифицировать личность, от конечных пользователей через cookies и другие технологии, вы должны обратиться за местной юридической рекомендацией о том, существуют ли какие-либо законы, применимые к такому сбору данных, включая все требования относительно предоставления замечаний и согласований.

Дополнительную информацию об использовании в этих целях различных технологий, включая cookies, смотрите на странице политики конфиденциальности IBM по адресу: http://www.ibm.com/privacy, и в заявлении IBM об электронной

конфиденциальности (IBM's Online Privacy Statement) по адресу: http://www.ibm.com/privacy/details, в разделе, озаглавленном "Cookies, Web Beacons and Other Technologies" (Cookies, веб-маяки и другие технологии), а также в документе "IBM Software Products and Software-as-a-Service Privacy Statement" ((Программные продукты IBM и заявление о конфиденциальности программ как услуг) по адресу: http://www.ibm.com/software/info/product-privacy.

Глоссарий

Есть глоссарий с терминами и определениями для семейства продуктов IBM Spectrum Protect.

См. IBM Spectrum Protect - Глоссарий.

Индекс

A

Aspera FASP 147, 148
Aspera Fast Adaptive Secure Protocol
    См. Aspera FASP
AUDIT CONTAINER 139

I

ID пользователя
    создать для сервера 50

L

LDAP
    требования к паролям 157

S

SSL 62

T

TLS 62

А

аппаратные средства хранения
    конфигурировать 39
аудит пула хранения 139

Б

брандмауэр 32, 33
брандмауэры
    конфигурирование связи через 128

В

веб-сервер
    остановка 111
    старт 111
внутреннее лицензирование мощности 103
восстановление
    журнал аварий 169
    стратегия 169
восстановление данных 167, 169, 171
    стратегия 169
восстановление поврежденных файлов
    репликация 175
второй сервер
    добавить как подчиненный сервер 79
    конфигурировать 77

Г

графический мастер
    необходимые файлы RPM 56

Д

данные
    деактивация 137
дедупликация данных
    конфигурировать 66
домены политик
    задать 118
доступ
    ограничение 159
    серверные опции 159

Е

ежедневный контрольный список задач мониторинга 85
емкость активного журнала 140
емкость архивного журнала 140
емкость базы данных 140
емкость перечня 140

Ж

журналы ошибок
    оценка 129

З

завершение работы
    сервер 161
задачи обслуживания
    запуск сервера в режиме обслуживания 162
    планирование 143
задачи переконфигурирования
    запуск сервера в режиме обслуживания 162
запланированные действия
    настройка 143
запуск сервера
    режим обслуживания 161
защита 153
защищенная связь
    конфигурирование SSL и TLS 62

И

использование процессора 142
исправить пул хранения
    поврежденные 176

К

Каталоги компонента IBM Spectrum Protect
    планирование 15
клавиатура 179
класс полномочий (privilege class)
    системные полномочия 156
клиенты
    выбор программы 116
    добавление 115
    защита 115

клиенты *(продолжение)*
конфигурирование 71, 123
конфигурирование для выполнения запланированных операций 125
назначить в расписания 71
обновление 133
определить расписания 70
перемещение 144
регистрация 122
регистрировать (register) 71
соединение с сервером 122
списание 144
управление операциями 129
установка 71, 123
команды
HALT 161
REPAIR STGPOOL 176
конфигурация
изменение 130
клиенты 123
конфигурация хранения
планирование 15
конфигурирование
клиенты 71
Подчиненный сервер 109

Л

лицензирование эффективных единиц процессора (Processor Value Unit, PVU) 103
лицензия на продукт
регистрировать (register) 66

М

мастер первоначального конфигурирования
конфигурировать 111
многонаправленный ввод-вывод
конфигурирование для систем AIX 47
конфигурирование для систем Linux 48
конфигурирование для систем Windows 49
мониторинг
ежедневный контрольный список 85
задачи
ежедневный контрольный список 85
периодический контрольный список 95
периодический контрольный список 95
цели 83

О

Об этой публикации v
обновление
сервер 165
обновление системы
prepare 167
обслуживание
определить расписание 67
ограничение
доступ пользователей 158
операции архивирования
задание правил 118
планирование 121
операции резервного копирования
задание правил 118
изменение области 132
операции резервного копирования *(продолжение)*
планирование 121
операционная система
защита 158
установка в серверных системах AIX 40
установка в серверных системах Linux 41
установка в серверных системах Windows 46
опции
задать для сервера 61
остановка
сервер 161
отключение
prepare 167
отработка восстановления 169
отчеты
электронная почта
конфигурирование 105
отчеты о состоянии
получить 105

П

пароли
изменение 157
сброс 131
периодический контрольный список задач мониторинга 95
планирование решений
диск с несколькими площадками 1
подчиненные серверы
восстановление до предварительно сконфигурированного состояния 113
Подчиненный сервер
remove 110
добавить 79
добавление 109
политики
задать 118
просмотр 119
редактирование 119
потеря данных 171
правила
задать
операции резервного копирования и архивирования 118
просмотр 119
редактирование 119
правила хранения данных
задать 67
приемник клиента (client acceptor)
конфигурирование 125
остановка 130
перезапуск 130
проблемы
диагностика 83
программная
выбор 116
пространство хранения
высвобождение 137
процесс деактивации
резервные данные 137
процесс списания
клиентский узел 134
публикации v
пулы хранения
контейнеры аудита 139

Р

рабочая таблица планирования 15
расписания
  операции резервного копирования и архивирования 121
реализация
  операции проверки 81
регистрация
  клиенты 122
режим обслуживания
  сервер запуска 161
репликация 79, 148
  изменить 150
  политики на сервере назначения 151
  разрешение 147
  решение с несколькими площадками
    совместимость 147
  управление 147
репликация узла
  включить 79
решение
  расширение 115
решение с несколькими площадками
  планирование 1

С

связь между клиентом и сервером
  конфигурирование 128
сервер
  включить политики назначения для репликации 151
  включить репликацию 147
  восстановление данных 175
  задать опции 61
  задать расписание обслуживания 67
  запуск в режиме обслуживания 161
  изменение репликации 150
  конфигурирование второго сервера 77
  конфигурировать 59
  обновление плана 165
  определение размера 3
  остановка 161
  репликация узла 147
  создать ID пользователя для 50
  управление репликацией 147
серверы
  запуск в режиме обслуживания 162
служба управления клиентом
  конфигурирование Центра операций 74
  проверка установки 73
  установка 72
соответствие лицензии
  проверка 103
состояние системы
  отслеживание 105
специальные возможности 179
способ восстановления
  потеря данных 171
  системное отключение электричества 171

Т

требования к аппаратным средствам 9
требования к памяти
  управление 142
требования к паролям
  LDAP 157
Требования к программному обеспечению
  Linux 11
требования к системе 9, 11
  аппаратная 9

У

узлы клиентов
  списание 134
  удаление из производства 134
управление
  администраторы 156
  полномочия (authority) 156
  уровни доступа 158
управление защитой 153
уровень полномочий 156
установить сервер
  Системы AIX 55
  Системы Linux 55
  Системы Windows 56
установка
  клиенты 71
установка операционной системы
  серверные системы AIX 40
  серверные системы Linux 41
  серверные системы Windows 46
установка сервера
  Системы AIX 55, 56
  Системы Linux 55, 56
установки
  клиенты 123
устранение неисправностей 83
  ID администратора 131
  заблокированные клиентские узлы 131
  ошибки в клиентских операциях 129
  ошибки паролей 131

Ф

файловые системы
  планирование 15
  подготовка, серверные системы AIX 51
  подготовка, серверные системы Linux 52
  подготовка, серверные системы Windows 53
файлы RPM
  установка для графического мастера 56
физические недостатки 179
фронтальное лицензирование мощности 103

Х

хаб-сервер
  восстановление до предварительно сконфигурированного
    состояния 113
  защищенная связь SSL 77
  изменение 112
хранение, пул
  защита 148
  исправить 148, 176

Ц

Центр знаний v
Центр знаний IBM v

Центр операций
веб-сервер 111
восстановление до предварительно сконфигурированного состояния 113
защищенная связь 63
конфигурировать 63
Подчиненный сервер 109

Э

электронные отчеты
конфигурирование 105

Номер программы: 5725-W98
5725-W99
5725-X15

Напечатано в Дании