

IBM Spectrum Protect
версия 8.1.7

*Введение в решения по
защите данных*



IBM Spectrum Protect
версия 8.1.7

*Введение в решения по
защите данных*



Примечание:

Прежде чем использовать эту информацию и описываемый в ней продукт, прочтите информацию в разделе “Замечания” на стр. 57.

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.

© Copyright IBM Corporation 1993, 2019.

Содержание

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

Часть 1. Понятия, связанные с IBM Spectrum Protect 1

Глава 1. IBM Spectrum Protect - Обзор	3
Компоненты защиты данных	3
Службы защиты данных	4
Процессы для управления защитой данных в IBM Spectrum Protect	7
Пользовательские интерфейсы для среды IBM Spectrum Protect.	11

Глава 2. Понятия, касающиеся хранения данных в IBM Spectrum Protect.	13
Типы устройств хранения	13
Хранение данных в пулах хранения.	17
Транспорт данных в пространство хранения в разных сетях	23

Глава 3. Стратегии защиты данных с использованием IBM Spectrum Protect 29	
Стратегии минимизации использования пространства хранения для резервных копий	29
Стратегии для защиты при авариях.	31
Стратегии для аварийного восстановления с использованием IBM Spectrum Protect	36

Часть 2. Решения IBM Spectrum Protect для защиты данных 39

Глава 4. Реализация решения по защите данных на основе дисков для одной площадки	41
---	-----------

Глава 5. Реализация решения по защите данных на основе дисков для нескольких площадок.	43
---	-----------

Глава 6. Реализация решения по защите данных на основе ленты	45
---	-----------

Глава 7. Реализация решения по защите данных на основе устройств для нескольких площадок.	47
--	-----------

Глава 8. Сравнение решений по защите данных	49
--	-----------

Глава 9. Дорожная карта для реализации решения по защите данных	51
--	-----------

Часть 3. Приложения 53

Приложение. Специальные возможности для семейства продуктов IBM Spectrum Protect	55
---	-----------

Замечания	57
----------------------------	-----------

Глоссарий	63
----------------------------	-----------

Индекс	65
-------------------------	-----------

Об этой публикации

В этой публикации представлен обзор концепций IBM Spectrum Protect и решений по защите данных, в которых используются наилучшие практические методы для IBM Spectrum Protect. Диаграмма сравнения компонентов поможет вам выбрать наилучшее решение, соответствующее требованиям вашей организации.

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 клиент-сервер. 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.

Часть 1. Понятия, связанные с IBM Spectrum Protect

IBM Spectrum Protect обеспечивает всеобъемлющую среду защиты данных.

Глава 1. IBM Spectrum Protect - Обзор

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

Компоненты защиты данных

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

Сервер

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

Перечень содержит следующие компоненты:

Database

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

Журнал восстановления

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

Системы и приложения клиентов

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

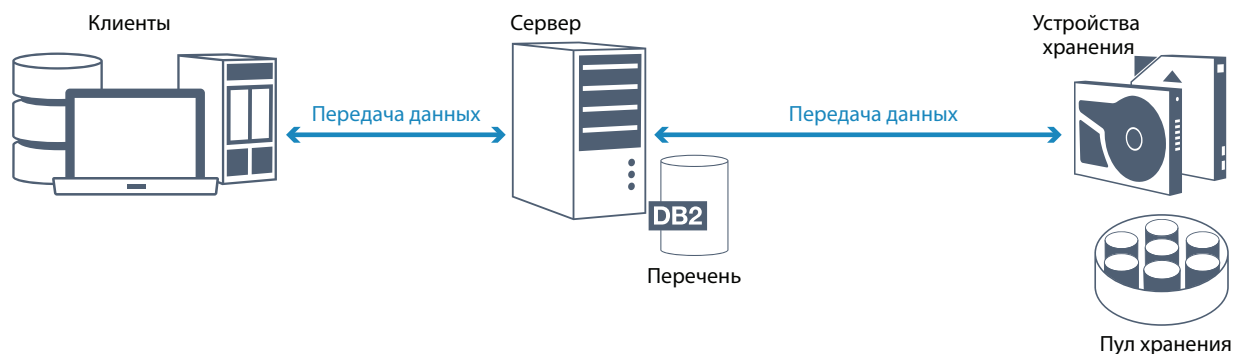


Рисунок 1. Компоненты в решении по защите данных

Программа клиента

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

Клиентские узлы

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

Носитель хранения

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

Устройства хранения

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

Пулы хранения

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

Службы защиты данных

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

Типы служб защиты данных

В IBM Spectrum Protect есть службы для сохранения и восстановления данных клиента, как показано на рис. 2 на стр. 5.

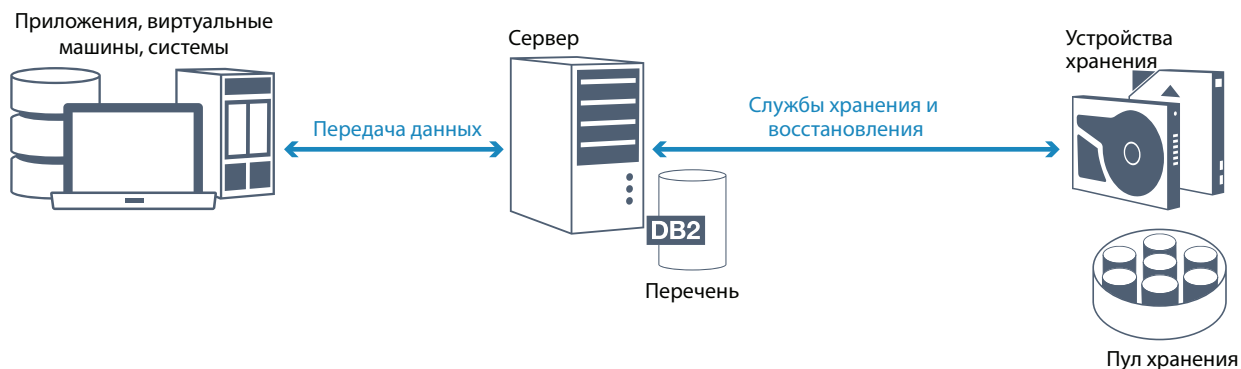


Рисунок 2. Службы защиты данных

В IBM Spectrum Protect есть следующие типы служб защиты данных:

Службы резервного копирования и восстановления

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

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

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

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

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

Службы архивирования и получения

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

- При архивировании данных вы указываете, сколько времени должны храниться данные.

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

Служба получения обеспечивает следующие возможности:

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

Службы переноса и возврата

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

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

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

Типы данных клиента, которые можно защитить

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

Клиенты приложения

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

- Клиенты IBM Spectrum Protect for Enterprise Resource Planning:
 - Data Protection for SAP HANA
 - Data Protection for SAP for Db2
 - Data Protection for SAP for Oracle
- Клиенты IBM Spectrum Protect for Databases:
 - Data Protection for Microsoft SQL Server
 - Data Protection for Oracle
- Клиенты IBM Spectrum Protect for Mail:
 - Data Protection for IBM Domino
 - Data Protection for Microsoft Exchange Server

Виртуальные машины

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

Клиенты компьютера

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

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

Процессы для управления защитой данных в IBM Spectrum Protect

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

Процесс управления данными

На рис. 3 показан процесс управления данными IBM Spectrum Protect.

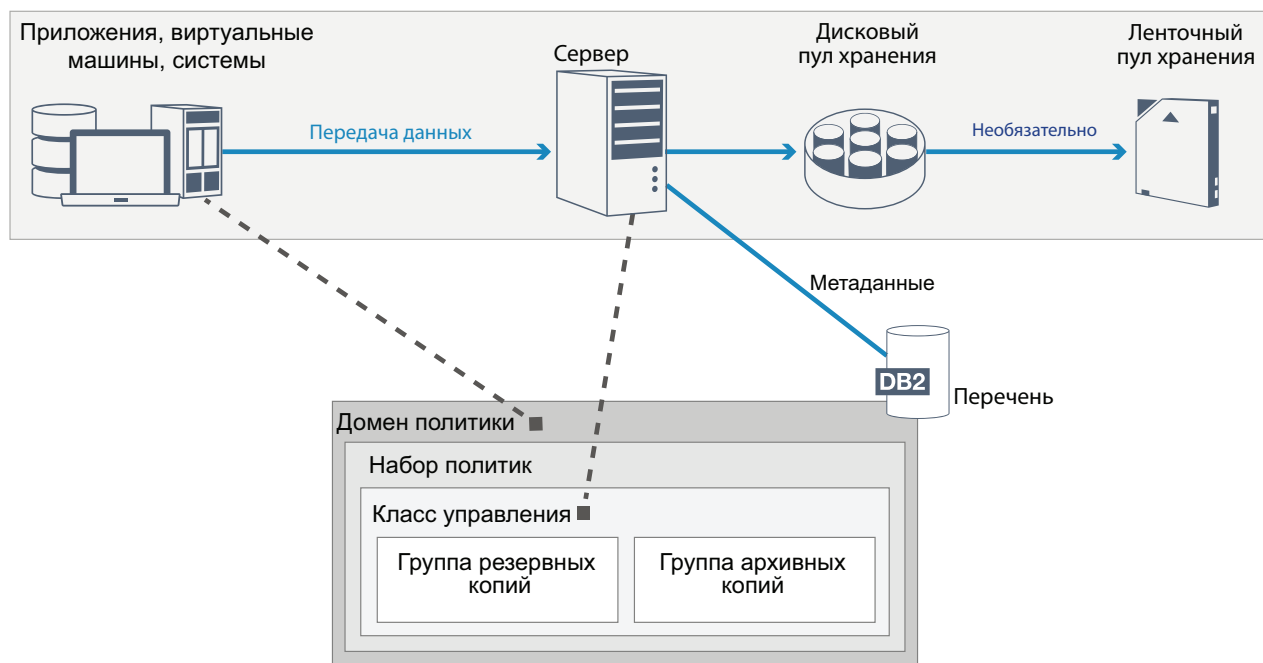


Рисунок 3. Процесс управления данными

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

Если вы настроили хранение сервера в иерархии, вы можете переносить файлы в разные пулы хранения.

Компоненты перечня

Перечисленные ниже компоненты перечня являются ключом к работе сервера:

База данных сервера

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

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

Журнал восстановления

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

Активный журнал

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

Зеркальная копия журнала (необязательно)

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

Архивный журнал

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

Резервный архивный журнал (необязательно)

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

Управление данными на основе политик

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

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

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

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

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

Вы создаете политики, задавая следующие компоненты политики:

Домен политики

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

Набор политик

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

Класс управления

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

В классе управления может содержаться группа резервных копий, группа архивных копий и атрибуты управления пространством. Группа копий определяет, как сервер управляет резервными версиями или архивными

копиями файла. Атрибуты управления пространством определяют, подлежит ли файл переносу клиентом менеджера по пространству в серверное хранилище и при каких условиях производится перенос файла.

Группа копирования

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

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

Управление защитой

IBM Spectrum Protect содержит ряд функций для регистрации администраторов и пользователей. После регистрации администраторов им нужно предоставить полномочия, назначив для них один или несколько классов административных полномочий. Администратор с системными полномочиями может выполнять на сервере любые функции. Администраторы, обладающие полномочиями на управление политиками, хранилищем, операторами или узлами, могут выполнять только определенное подмножество функций сервера. Доступ к серверу можно получить следующими способами, каждый из которых управляется паролем:

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

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

Открытая регистрация

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

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

Закрытая регистрация

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

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

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

Пользовательские интерфейсы для среды IBM Spectrum Protect.

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

Интерфейсы для управления хранением данных

Центр операций - это основной интерфейс для администраторов, позволяющий производить мониторинг и администрирование серверов. Важнейшее преимущество центра операций в том, что можно производить мониторинг нескольких серверов, как показано на рис. 4. Также можно производить мониторинг и администрирование IBM Spectrum Protect из административного интерфейса командной строки.

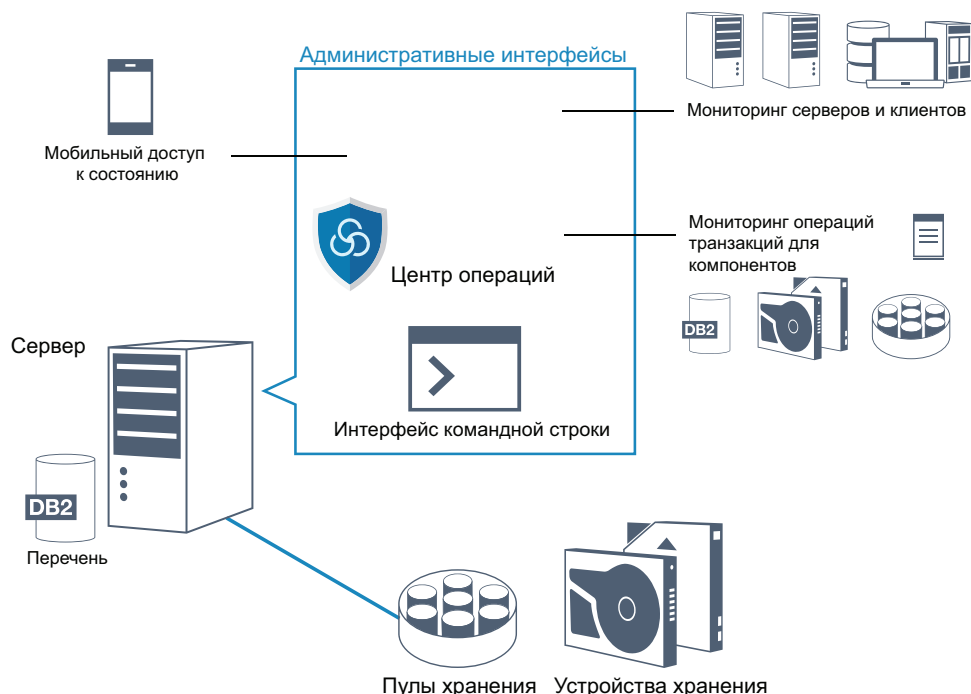


Рисунок 4. Интерфейсы пользователя для управления хранением данных

Для взаимодействия с IBM Spectrum Protect можно использовать следующие интерфейсы:

Центр операций

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

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

Интерфейс командной строки

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

Доступ к информации в базе данных сервера с использованием операторов SQL

Операторы SQL SELECT можно использовать, чтобы запрашивать базу данных сервера и просматривать результаты. Существуют инструменты SQL сторонних поставщиков, помогающие администраторам управлять базами данных.

Интерфейсы для управления операциями клиентов

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

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

Глава 2. Понятия, касающиеся хранения данных в IBM Spectrum Protect

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

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

Типы устройств хранения

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

Устройства хранения и объекты хранения

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

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

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

Таблица 1. Объекты хранения, и что они представляют

Объект хранения	Что представляет объект
Том	Дискретный блок хранения на диске, ленте или на другом носителе хранения. Каждый том связан с одним пулом хранения.
Пул хранения	Набор томов или контейнеров хранения, которые служат пунктом назначения для хранения данных клиентов. IBM Spectrum Protect использует следующие типы пулов хранения: <ul style="list-style-type: none">• Пулы хранения контейнеров каталогов• Пулы хранения облачных контейнеров• Пулы хранения с последовательным доступом, связанные с классом устройств• Пулы хранения с произвольным доступом, связанные с классом устройств
Контейнер	Место хранения данных, например, файл, каталог или устройство.

Таблица 1. Объекты хранения, и что они представляют (продолжение)

Объект хранения	Что представляет объект
Пул хранения контейнера	Первичный пул хранения, используемый сервером для хранения данных. Данные хранятся в контейнерах в каталогах файловой системы или в облачном хранилище. Если потребуется, производится дедупликация данных, когда сервер записывает данные в пул хранения.
Класс устройств	Тип устройства хранения, которое может использовать тома, заданные для пула хранения с последовательным или произвольным доступом. Каждый класс устройств типа Съёмный носитель связан с одной библиотекой.
Библиотека	Устройство хранения. Например, библиотека может представлять автономный накопитель, набор автономных накопителей, автоматизированное устройство с несколькими накопителями или набор накопителей, которые управляются менеджером носителей.
Накопитель	Объект устройства ленточной библиотеки, обеспечивающий возможность читать и записывать данные на ленточный носитель библиотеки. Каждый накопитель связан с одной библиотекой.
Путь	Спецификация источника данных и назначения устройства. Прежде чем можно будет использовать устройство хранения, должен быть задан путь между устройством и исходным сервером, выполняющим перемещение данных.
Узел перемещения данных	Подключенное к SAN устройство, которое используется для передачи данных клиента. Узел перемещения данных используется только при передаче данных, в которой не участвует сервер (например, среда Network Data Management Protocol - NDMP). Средства перемещения данных выполняют обмен данными между устройствами хранения, не используя значительного количества ресурсов сервера, клиента или сети.
Сервер	Сервер, который управляется другим сервером IBM Spectrum Protect.

Администратор задает объекты хранения на логическом уровне сервера, как показано на рис. 5 на стр. 15.

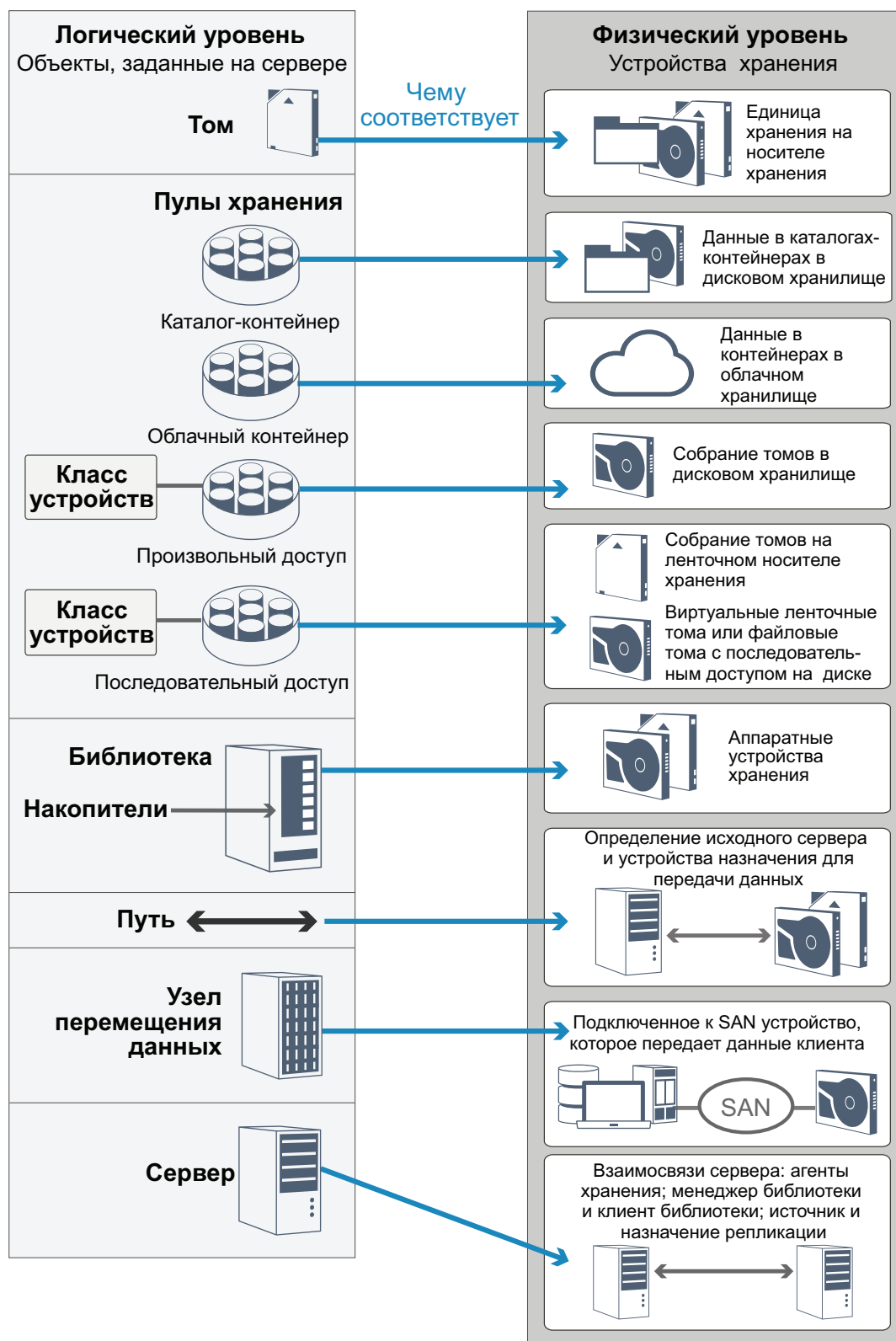


Рисунок 5. Объекты хранения

Дисковые устройства

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

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

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

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

Физические ленточные устройства

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

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

Перемещение данных на ленту обеспечивает следующие преимущества:

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

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

Виртуальные ленточные библиотеки

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

Если задать VTL на сервере IBM Spectrum Protect, при этом может повыситься производительность, так как сервер выполняет обработку точек монтирования для библиотек VTL иначе, чем для реальных ленточных библиотек. Хотя логические

ограничения ленточных устройств все равно остаются, физические ограничения для ленточного оборудования неприменимы к VTL, обеспечивая более высокую масштабируемость. IBM Spectrum Protect VTL можно использовать, если выполнены следующие условия:

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

Хранение данных в пулах хранения

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

Типы пулов хранения

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

Первичные пулы хранения

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

Пулы хранения копий

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

Пулы хранения контейнера-копии

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

Пулы хранения активных данных

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

Первичные пулы хранения

При восстановлении, получении, возврате или экспорте файла данных затребованный файл берется из первичного пула хранения. В зависимости от типа первичного пула хранения пулы хранения данных могут находиться на площадке или вне площадки. Первичные пулы хранения можно организовать в виде иерархии хранения, чтобы данные можно было переносить из дискового пространства хранения в более экономичное пространство хранения, например, на ленточные устройства. На рис. 6 на стр. 18 проиллюстрировано понятие первичных пулов хранения.

Первичные пулы хранения

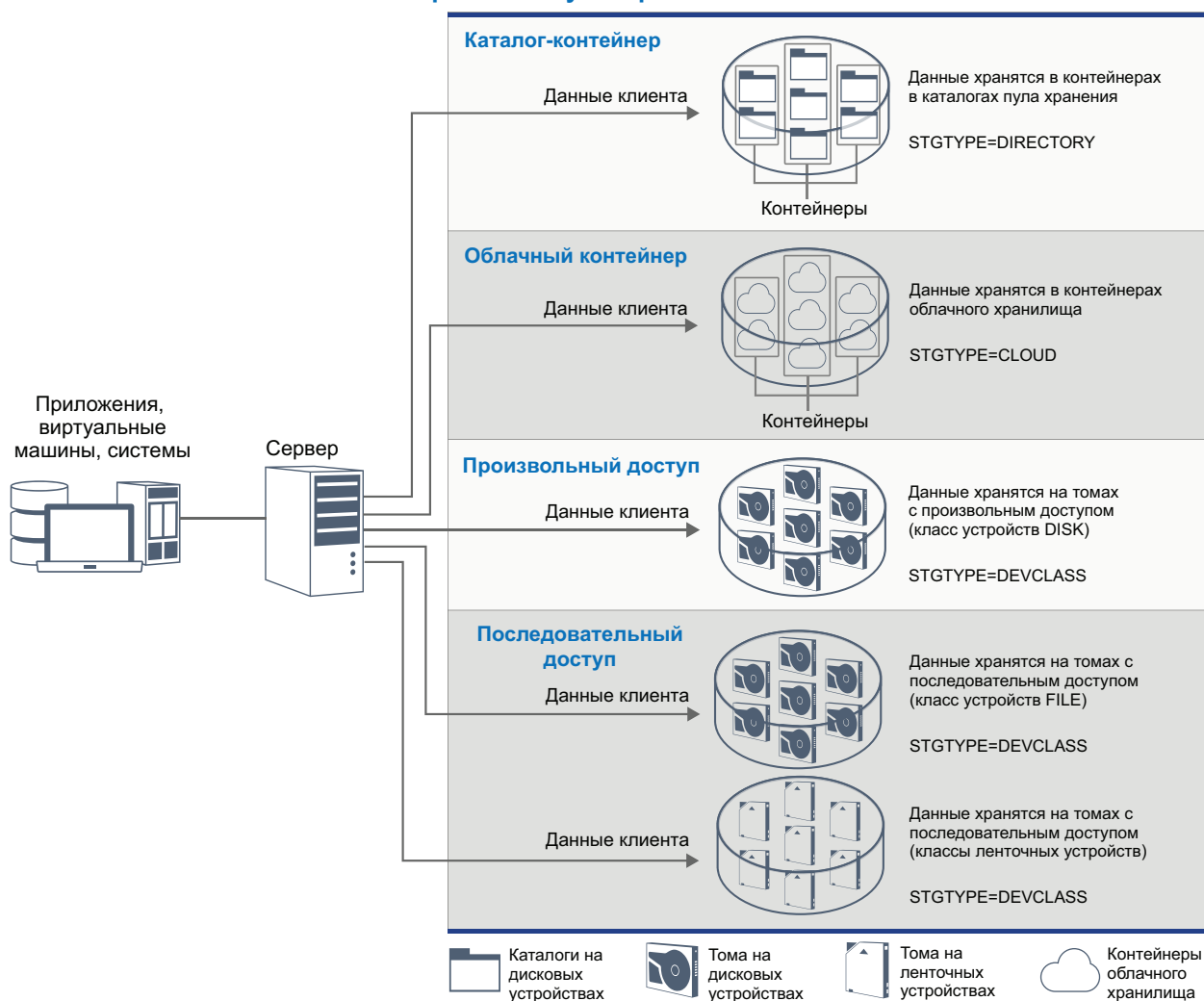


Рисунок 6. Первичные пулы хранения

Можно задать следующие типы первичных пулов хранения:

Пулы хранения контейнеров каталогов

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

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

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

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

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

Пулы хранения облачных контейнеров

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

Можно задать следующие типы пулов хранения облачных контейнеров:

На месте

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

Вне системы

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

Пулы хранения, связанные с классами устройств

Вы можете задать первичный пул хранения, чтобы использовать следующие типы устройств хранения:

Класс устройств DISK

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

Класс устройств FILE

В случае типа устройств FILE в пуле хранения файлы хранятся на последовательных томах, чтобы обеспечить более высокую производительность последовательного доступа, чем при хранении на дисковых блоках. Для сервера эти файлы будут иметь характеристики ленточного тома, поэтому такой тип пула хранения лучше подходит для переноса на ленту. Тома FILE полезны как *электронное хранилище*, когда данные передаются на удаленную площадку по электронной сети, а не путем физической поставки ленты. В общем случае, этот тип пула хранения является более предпочтительным, чем пулы хранения DISK.

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

ARCHIVEPOOL

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

BACKUPPOOL

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

SPACEMGPOOL

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

Пулы хранения копий

В пулах хранения копий содержатся активные и неактивные версии данных, резервные копии которых были созданы на основе данных в первичных пулах хранения. Пул хранения каталога-контейнера нельзя использовать как пул хранения копий. Кроме того, данные из пула хранения каталога-контейнера нельзя скопировать в пул хранения копий. Для защиты пулов хранения каталогов-контейнеров скопируйте данные в пул хранения контейнеров-копий. На рис. 7 на стр. 21 проиллюстрировано понятие пулов хранения копий.

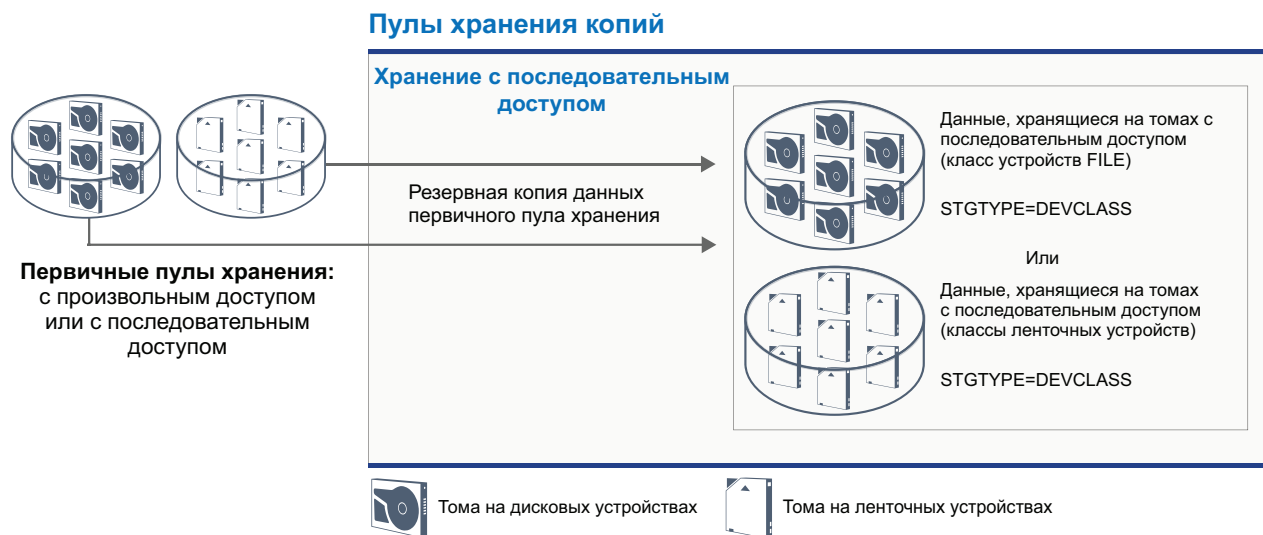


Рисунок 7. Пулы хранения копий

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

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

Пулы хранения контейнера-копии

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

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

- С помощью репликации можно восстанавливать данные клиента непосредственно с сервера назначения, если исходный сервер недоступен.

- Работая с пулами хранения контейнеров-копий, надо сначала восстановить сервер из резервной копии базы данных и затем исправить пулы хранения каталогов-контейнеров с ленточных устройств.

На рис. 8 проиллюстрировано понятие пулов хранения контейнеров-копий.



Рисунок 8. Пулы хранения контейнера-копии

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

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

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

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

Пулы хранения активных данных

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

- Повысить скорость операций восстановления данных клиента
- Сократить число томов хранения на месте или вне системы

- Сократить объем данных, передаваемых при копировании или восстановлении файлов, хранящихся в электронном виде на удаленной площадке

В пулах активных данных не могут находиться файлы, перенесенные клиентами управления иерархическим хранилищем, равно как и архивные файлы. Поскольку обновленные версии резервных копий данных хранятся в пулах активных данных, более старые версии удаляются, так как оставшиеся данные консолидируются с многих томов с последовательным доступом на меньшее число новых томов с последовательным доступом. На рис. 9 проиллюстрировано понятие пулов хранения активных данных.



Рисунок 9. Пулы хранения активных данных

Для создания пулов активных данных можно использовать любые типы пространства хранения с последовательным доступом. Однако преимущества пула активных данных зависят от типа устройств, связанного с пулом. Например, для операций быстрого восстановления клиентов идеально подходят пулы активных данных, связанные с классом устройств FILE, по следующим причинам:

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

Транспорт данных в пространство хранения в разных сетях

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

Конфигурации сети для устройств хранения

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

Операции резервного копирования данных через LAN

На рис. 10 показан путь данных для операций резервного копирования IBM Spectrum Protect через LAN.

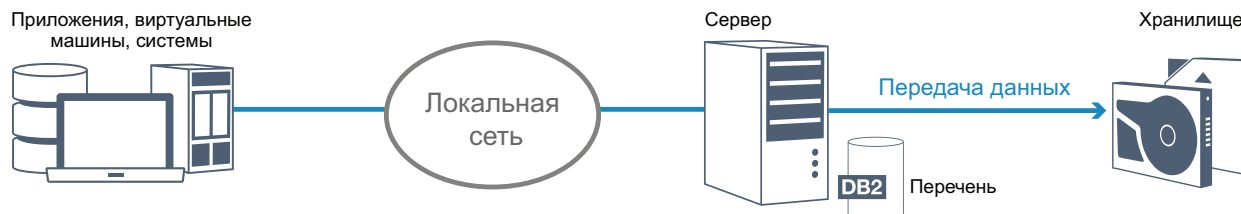


Рисунок 10. Операции резервного копирования IBM Spectrum Protect через LAN

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

Операции резервного копирования данных через SAN

На рис. 11 показан путь данных для операций резервного копирования IBM Spectrum Protect через SAN.

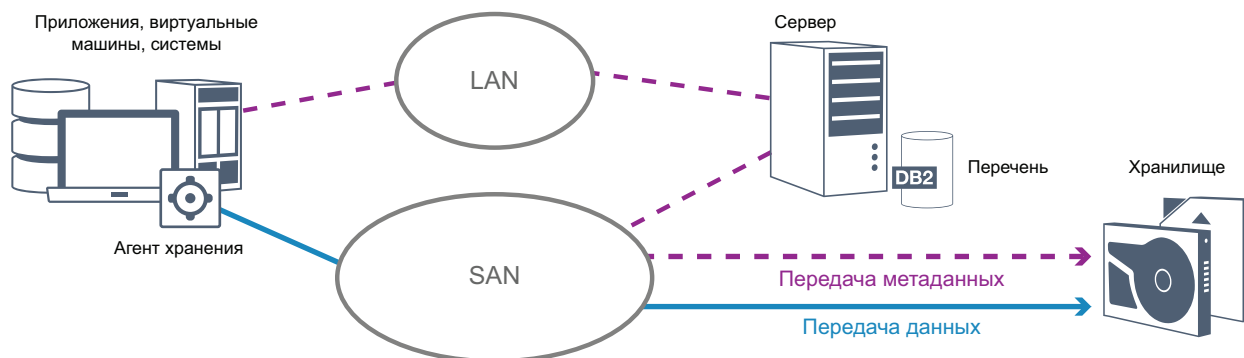


Рисунок 11. Операции резервного копирования IBM Spectrum Protect через SAN

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

- Совместное использование устройств хранения несколькими серверами IBM Spectrum Protect. Устройства, использующие тип устройств GENERICTAPE, не включаются.
- Переместите данные из системы клиента непосредственно на устройства хранения, не используя локальную сеть. Перемещение данных в режиме без локальной сети требует установки агента хранения на клиентской системе. Агент хранения прилагается к продукту IBM Spectrum Protect for SAN.

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

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

Хранилище NAS

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

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

Управление хранением

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

Типы устройств для серверного хранилища

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

Перенос данных в иерархии хранения

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

Удаление устаревших данных

Заданная политика определяет, когда должен заканчиваться срок хранения данных на сервере IBM Spectrum Protect. Для удаления данных с истекшим сроком хранения серверный процесс помечает их как данные, срок хранения которых истек, и удаляет из базы данных соответствующие метаданные. Теперь место, которое занимали такие данные, доступно для хранения новых данных. Вы можете управлять частотой выполнения процесса обработки данных с истекшим сроком хранения, используя соответствующую серверную опцию.

Повторное использование носителей за счет их освобождения

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

Консолидация резервных копий данных клиента

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

Совместное размещение данных клиентов

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

потребуется выделенный том вместо того, чтобы данные с нескольких клиентов хранились на одном и том же томе.

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

Связывание пулов активных данных с различными устройствами

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

Создание набора резервных копий

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

Перемещение данных на клиентский узел

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

Глава 3. Стратегии защиты данных с использованием IBM Spectrum Protect

IBM Spectrum Protect обеспечивает возможность реализовать различные стратегии защиты данных.

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

Стратегии минимизации использования пространства хранения для резервных копий

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

Дедупликация данных

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

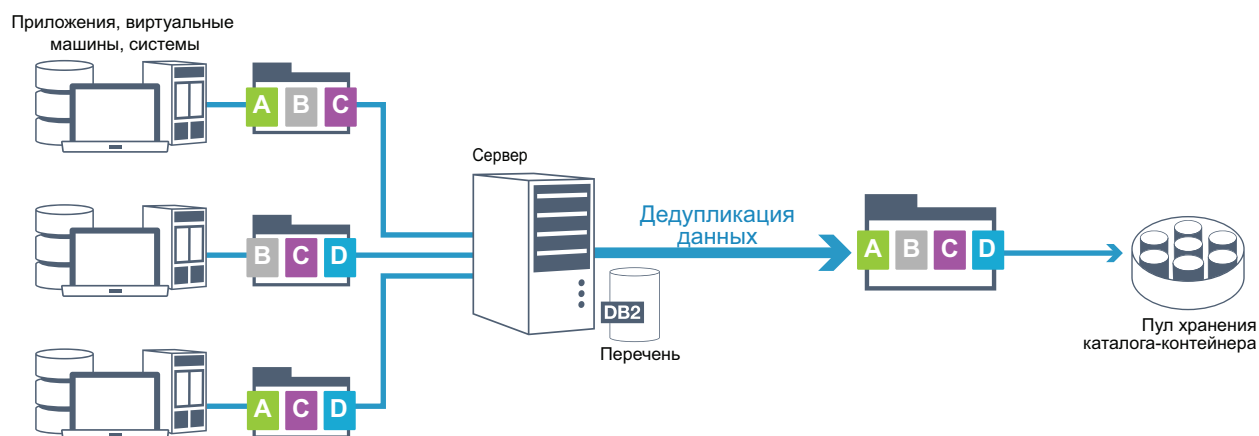


Рисунок 12. Процесс дедупликации данных

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

IBM Spectrum Protect обеспечивает следующие типы дедупликации данных:

Дедупликация данных на стороне сервера

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

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

Дедупликация данных на стороне клиента

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

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

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

Сжатие

Используйте встроенное сжатие, чтобы сократить объем пространства в пулах хранения контейнеров. Данные сжимаются при их записи в пул хранения контейнера.

Ограничение: Сервер IBM Spectrum Protect не может сжимать зашифрованные данные.

Прогрессивное инкрементное резервное копирование

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

Стратегии для защиты при авариях

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

Репликация на удаленной площадке

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

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

Преимущества

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

Недостатки

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

На рис. 13 на стр. 32 показан процесс репликации узла на удаленной площадке.

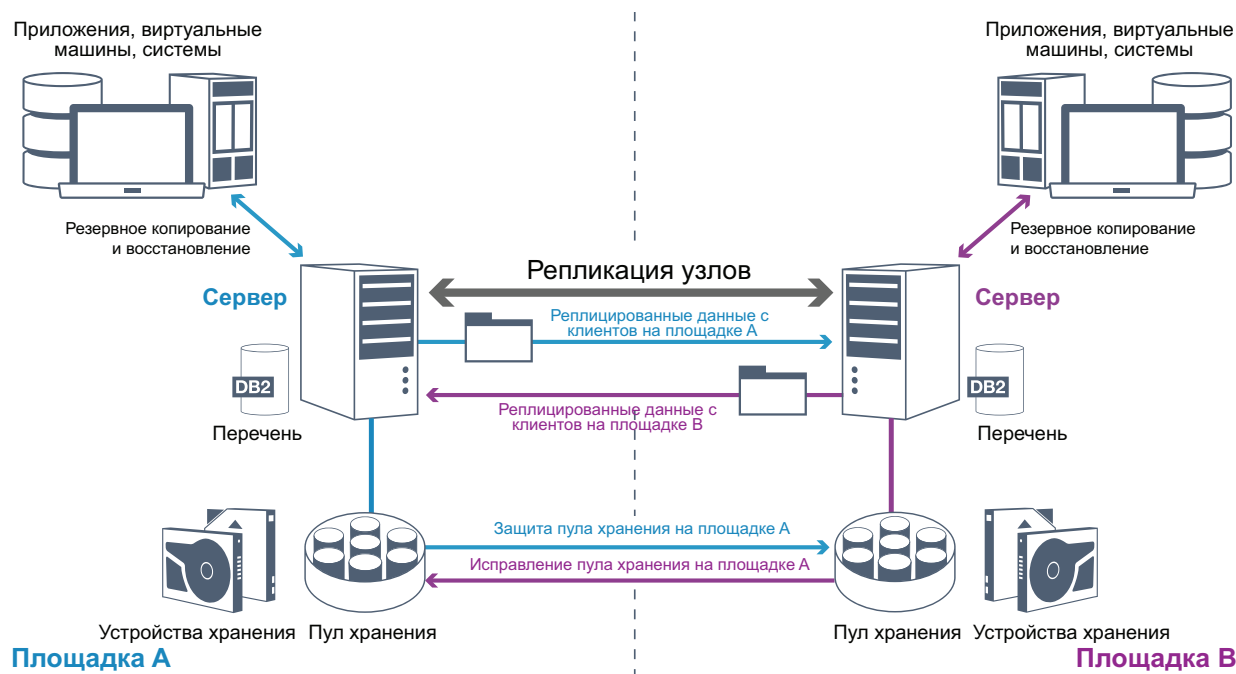


Рисунок 13. Процесс репликации узла

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

IBM Spectrum Protect обеспечивает следующие функции репликации:

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

Если произойдет авария и исходный сервер окажется недоступен, клиенты смогут восстановить данные с целевого сервера. Если исходный сервер восстановить невозможно, вы можете направить клиенты для сохранения данных на целевом сервере. В случае перебоя с питанием клиента, которые производили резервное копирование на исходный сервер, смогут автоматически передать управление для восстановления данных с сервера назначения (целевого сервера).

- Вы можете использовать обработку репликации для восстановления поврежденных файлов из пулов хранения. Нужно реплицировать данные клиента на целевом сервера до повреждения файлов. Последующие процессы репликации обнаруживают поврежденные файлы на исходном сервере и заменяют файлы неповрежденными файлами с целевого сервера.

Роль репликации в защите в случае аварии

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

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

Защита пула хранения

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

Преимущества

- Быстрое восстановление и перестройка исходной системы.

Недостатки

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

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

Пулы хранения контейнеров каталогов

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

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

Пулы хранения контейнера-копии

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

Пулы хранения, связанные с классами устройств FILE и DISK

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

Резервные копии базы данных

Вы используете резервные копии базы данных для восстановления системы после повреждения базы данных. Кроме того, нужно использовать операции резервного копирования базы данных, чтобы не дать Db2 исчерпать пространство архивного журнала. Операции резервного копирования базы данных не являются частью репликации узлов. Резервные копии базы данных могут содержать полные или инкрементные резервные копии, а также копии, выполненные в режиме снимка. Чтобы обеспечить возможность аварийного восстановления, нужно хранить резервные копии базы данных вне сайта. Для восстановления базы данных необходимы тома резервных копий базы данных. Вы можете восстановить базу данных с томов резервных копий либо путем восстановления моментального снимка, либо с помощью операции самого актуального восстановления.

Восстановление на заданный момент времени

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

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

Восстановление до самого последнего состояния

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

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

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

Альтернативные методы защиты от аварий

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

Отправка лент с резервными копиями на удаленную площадку

Резервные копии данных создаются на ленте исходным сервером в

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

Репликация устройств с несколькими площадками на резервный сервер

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

Сравнение стратегий конфигурации защиты

Рассмотрим следующие возможные сценарии потери данных:

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

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

Конфигурации только для защиты от повреждений

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

Конфигурации для восстановления после аварий и защиты от повреждений

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

Стратегии для аварийного восстановления с использованием IBM Spectrum Protect

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

Автоматическая передача управления для аварийного восстановления

Автоматическая передача управления - это операция, которая переключается на резервную систему, если происходит прерывание программы, оборудования или сети. Автоматическая передача управления при отказе используется в сочетании с репликацией узлов для восстановления данных после системного сбоя. На рис. 14 показан процесс автоматической передачи управления IBM Spectrum Protect при отказе.

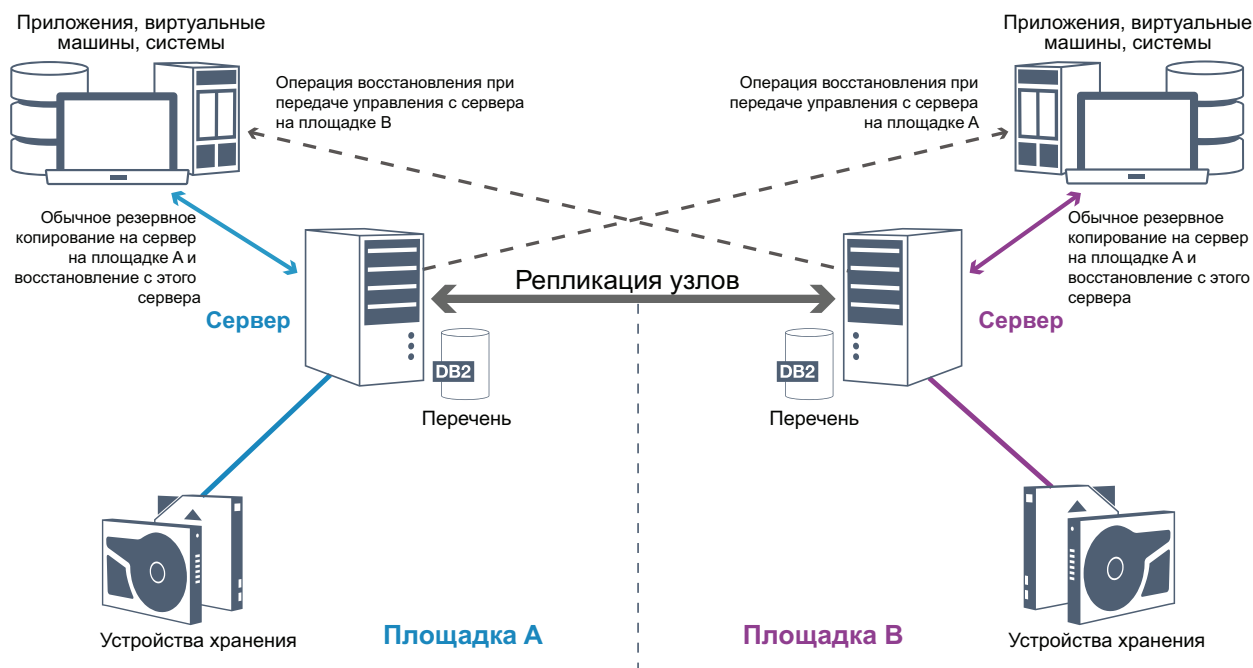


Рисунок 14. Процесс автоматической передачи управления при отказе

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

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

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

Восстановление компонентов IBM Spectrum Protect

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

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

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

- После первоначального полного резервного копирования пулов хранения каждую ночь выполняется инкрементное резервное копирование.
- Инкрементное резервное копирование базы данных выполняется каждую ночь.
- Полное резервное копирование базы данных выполняется раз в неделю.

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

Профилактические действия по восстановлению

Для восстановления применяются следующие профилактические действия:

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

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

- Создание плана аварийного восстановления для сервера

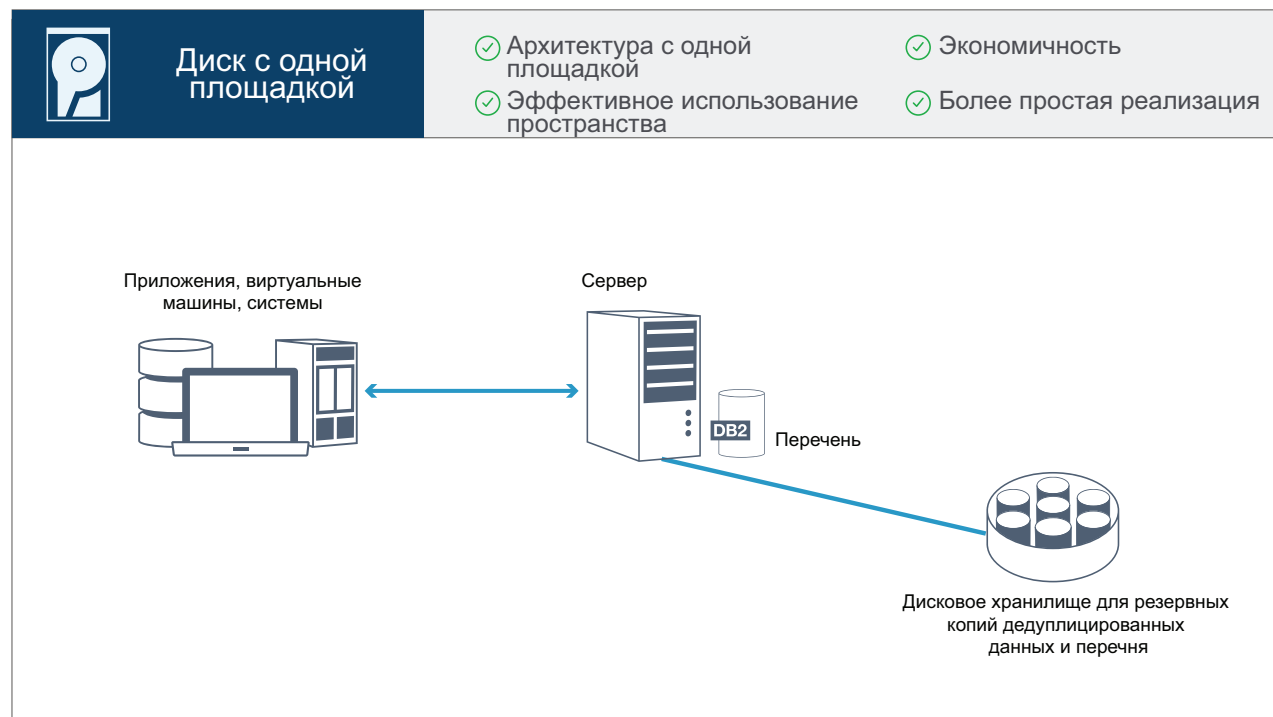
- Резервное копирование данных сервера на ленту
- Отправка данных резервных копий сервера на удаленную площадку или на другой сервер
- Хранение данных о клиентской системе
- Назначение и отслеживание носителей, используемых для сохранения и восстановления данных клиента

Часть 2. Решения IBM Spectrum Protect для защиты данных

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

Глава 4. Реализация решения по защите данных на основе дисков для одной площадки

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



Это решение по защите данных предоставляет следующие преимущества:

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

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

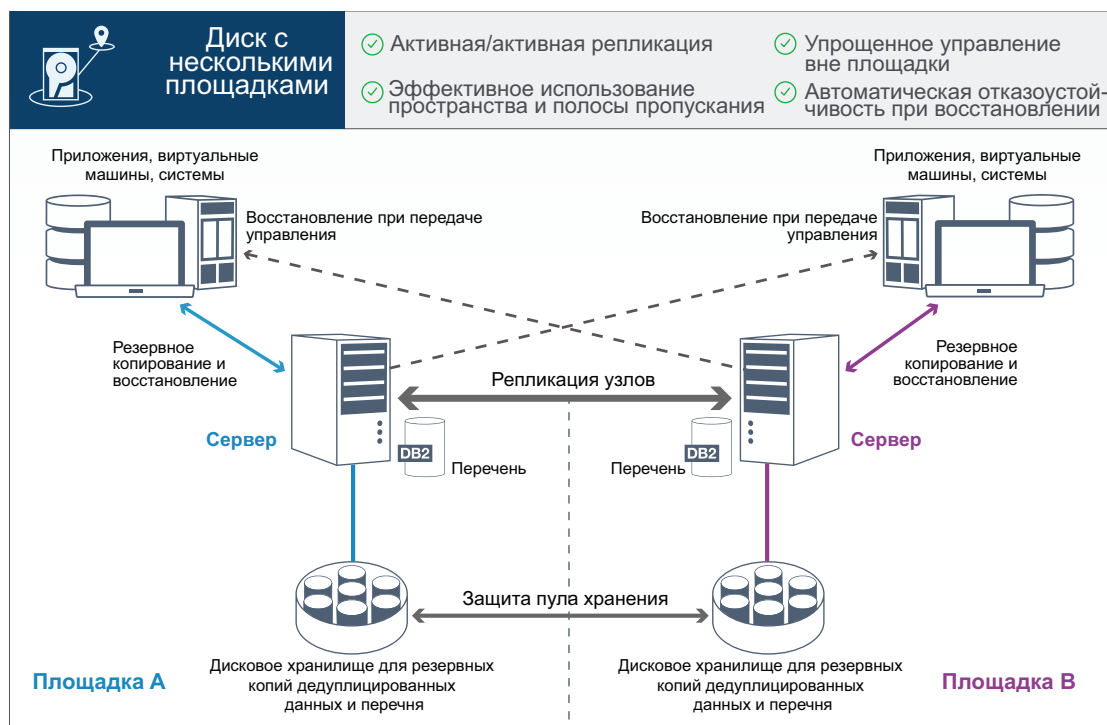
Ссылки, связанные с данной:

Глава 8, “Сравнение решений по защите данных”, на стр. 49

Глава 9, “Дорожная карта для реализации решения по защите данных”, на стр. 51

Глава 5. Реализация решения по защите данных на основе дисков для нескольких площадок

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



Это решение по защите данных предоставляет следующие преимущества:

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

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

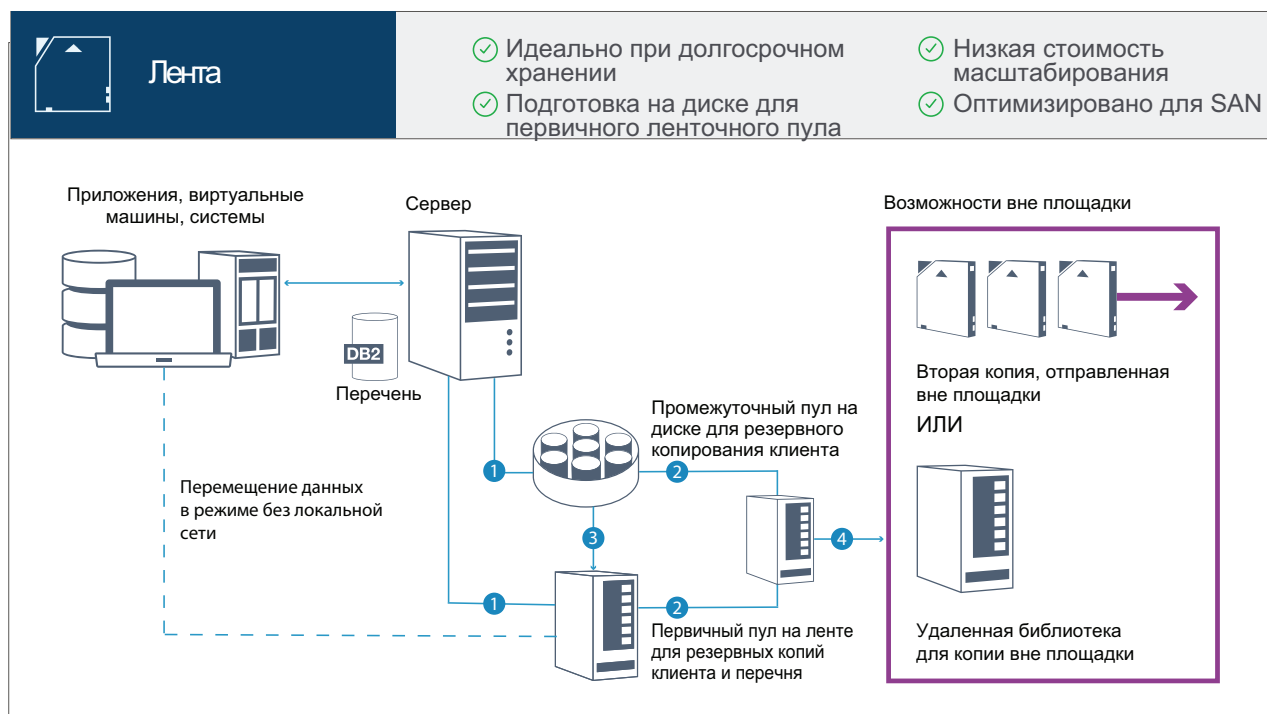
Ссылки, связанные с данной:

Глава 8, “Сравнение решений по защите данных”, на стр. 49

Глава 9, “Дорожная карта для реализации решения по защите данных”, на стр. 51

Глава 6. Реализация решения по защите данных на основе ленты

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



Это решение по защите данных предоставляет следующие преимущества:

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

Ссылки, связанные с данной:

Глава 8, "Сравнение решений по защите данных", на стр. 49

Глава 7. Реализация решения по защите данных на основе устройств для нескольких площадок

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



Это решение по защите данных предоставляет следующие преимущества:

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

При такой конфигурации защиты данных сервер использует аппаратные устройства для дедупликации и репликации данных. Устройство на площадке А дедуплицирует данные, а затем реплицирует данные на устройство на площадке В для защиты от

аварий. Если на площадке A произойдет сбой, вы сделаете резервный сервер активным, восстановив самую последнюю резервную копию базы данных и активировав реплицированную копию данных.

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





Ссылки, связанные с данной:





Глава 8, “Сравнение решений по защите данных”, на стр. 49

Глава 9, “Дорожная карта для реализации решения по защите данных”, на стр. 51

Глава 8. Сравнение решений по защите данных

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

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

	Диск с одной площадкой	Диск с несколькими площадками	Устройство с несколькими площадками	Лента
				
Возможность создания копий вне системы		✓	✓	✓
Репликация на основе устройств			✓	
Восстановление клиента с сервера высокой доступности		✓		
Пункт назначения репликации в облаке		✓		
Независимое управление политиками хранения для данных репликации; возможность сохранять больше или меньше данных на площадке восстановления		✓		
Репликация на уровне приложений; возможность выбрать, какие системы и приложения реплицируются		✓		
Масштабируемость				
Глобальная дедупликация данных на разных серверах			✓	
Оптимизированное для SAN резервное копирование непосредственно на ленту для типов данных больших объемов				✓
Масштабируемость в петабайтах для одного экземпляра				✓

Что делать дальше

Прочтите доступную документацию для решений в разделе Глава 9, “Дорожная карта для реализации решения по защите данных”, на стр. 51.

Ссылки, связанные с данной:

Глава 4, “Реализация решения по защите данных на основе дисков для одной площадки”, на стр. 41

Глава 5, “Реализация решения по защите данных на основе дисков для нескольких площадок”, на стр. 43

Глава 7, “Реализация решения по защите данных на основе устройств для нескольких площадок”, на стр. 47

Глава 6, “Реализация решения по защите данных на основе ленты”, на стр. 45

Глава 9. Дорожная карта для реализации решения по защите данных

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

Решение с одной площадкой

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

Решение с несколькими площадками

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

Решение на лентах

Шаги, в которых описано, как спланировать, реализовать, отслеживать и управлять решением с ленточным устройством, смотрите в разделе Решение на лентах.

Решение на основе устройств с несколькими площадками

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

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

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

7. Настройте мониторинг своей системы. Ознакомьтесь с информацией в разделе Мониторинг решений по хранению.

Ссылки, связанные с данной:

Глава 8, “Сравнение решений по защите данных”, на стр. 49

Глава 4, “Реализация решения по защите данных на основе дисков для одной площадки”, на стр. 41

Глава 5, “Реализация решения по защите данных на основе дисков для нескольких площадок”, на стр. 43

Глава 7, “Реализация решения по защите данных на основе устройств для нескольких площадок”, на стр. 47

Глава 6, “Реализация решения по защите данных на основе ленты”, на стр. 45

Часть 3. 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 ТТУ для использования глухими или слабо слышащими заказчиками с целью получения доступа к службам продаж и поддержки:

Служба ТТУ
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

А

API

См. интерфейс прикладного программирования

А

архитектура SAN 31, 36

Б

библиотека 13

В

веб-интерфейс клиента резервного копирования и архивирования 11

виртуальные машины 4

восстановление

данные 36

системные компоненты 36

встроенная дедупликация данных (inline data deduplication) 29

Г

графический пользовательский интерфейс для клиентов 11

Д

дедупликация данных

встроенная 29

сторона клиента 29

сторона сервера 29

Ж

журнал

активный журнал 7

архивный журнал 7

журнал восстановления 7

зеркальная копия журнала 7

резервный архивный журнал 7

журнал аварий

DRM 36

автоматическая передача управления 36

менеджер 36

профилактические меры 36

способы 31

журнал восстановления 7

З

защита данных

стратегии 29

И

интерфейс командной строки 11

интерфейс прикладного программирования 11

интерфейсы

API 11

графический пользовательский интерфейс клиента 11

клиент резервного копирования-архивирования
(backup-archive client) 11

командная строка 11

операторы SQL 11

Центр операций 11

К

клавиатура 55

класс устройства 13

клиентские данные

консолидация 23

переместить в пространство хранения 23

перенос 23

создать набор резервных копий 23

управление 23

клиенты

виртуальные машины 4

клиенты системы 4

приложения 4

принципы 3

программа клиента 3

типы 4

узлы клиентов 3

клиенты системы 4

клиенты-приложения 4

Л

ленточные устройства

виртуальный 13

физический 13

Н

накопитель 13

носители

рекламация 23

носитель, сменный 13

О

Об этой публикации v

операторы SQL для доступа к базе данных сервера 11

операционные системы 4

основные пулы хранения 17

П

передача управления, автоматическая 36

перечень 7

- политика
 - домен политики (policy domain) 7
 - набор правил политики (policy set) 7
 - стандартное 7
 - управление данными 7
- принципы
 - база данных 3
 - журнал восстановления 3
 - клиенты 3
 - обзор 3
 - перечень 3
 - сервер 3
 - хранение 3
- прогрессивное инкрементное резервное копирование 29
- публикации v
- пулы активных данных 23
- пулы контейнерного хранения 29
- пулы хранения
 - архивные данные 17
 - контейнер (container) 17, 29
 - копировать 17
 - копия контейнера 17
 - облако 17
 - первичный 17
 - представление 17
 - типы 17
- пулы хранения активных данных 17
- пулы хранения каталогов-контейнеров 17
- пулы хранения контейнера-копии 17
- пулы хранения копий 17
- пулы хранения облачных контейнеров 17
- путь (path) 13

Р

- репликация
 - исходный сервер 31
 - роль при восстановлении после аварии 31
 - сервер назначения 31
 - узел 31
- репликация узла 31, 36
- репликация устройств 31, 36
- решения
 - решение с несколькими площадками
 - на основе устройств 47
 - решения по защите данных
 - на основе устройств 47
- Решения IBM Spectrum Protect
 - решение с несколькими площадками
 - на основе диска 43
 - решение с одной площадкой
 - на основе диска 41
 - решения по защите данных 45
 - диск с несколькими площадками 43
 - диск с одной площадкой 41
 - сравнение 49
 - указатель информации 51

С

- сервер 13
 - журнал восстановления 7
 - перечень 7
 - принципы 3
 - склады данных 7

- сеть, типы
 - LAN 23
 - NAS 23
 - SAN 23
 - Режим без локальной сети 23
 - Хранилище nAS 23
- служба архивирования 4
- служба возврата 4
- служба восстановления 4
- служба переноса 4
- служба получения 4
- служба резервного копирования 4
- службы
 - архивирование и получение 4
 - перенос и возврат 4
 - резервное копирование и восстановление 4
- службы защиты данных 4
- совместное размещение 23
- специальные возможности 55

Т

- том (volume) 13
- тома 17
- транспорт лент 31, 36

У

- управление защитой
 - SSL 7, 23
 - TLS 7, 23
 - закрытая регистрация (closed registration) 7, 23
 - открытая регистрация (open registration) 7, 23
 - пароли 7, 23
- уровень
 - логический 13
 - физический 13
- устройство перемещения данных 13

Ф

- физические недостатки 55

Х

- хранение
 - иерархия 3, 23
 - объекты 13
 - поддержка устройств 23
 - представления 13
 - принципы 3
 - пулы 3, 13, 17
 - сети 23
 - типы 13
 - тома 17
 - управление 23
 - устройства 3, 13

Ц

- Центр знаний v
- Центр знаний IBM v
- Центр операций
 - доступ 11
 - функции 11



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

Напечатано в Дании