IBM Spectrum Protect for Virtual Environments
версия 8.1.7

Data Protection for VMware: Руководство по установке

IBM Spectrum Protect for Virtual Environments
версия 8.1.7

Data Protection for VMware: Руководство по установке

Примечание:

Прежде чем использовать эту информацию и описываемый в ней продукт, прочтите информацию в разделе “Замечания” на стр. 133.

Данное издание относится к версии 8, выпуску 1, модификации 7 IBM Spectrum Protect for Virtual Environments (номер продукта 5725-X00) и ко всем его последующим выпускам и модификациям, пока в новых изданиях не будет указано иное.

Содержание

Об этой публикации

Компонент IBM Spectrum Protect for Virtual Environments обеспечивает инкрементное резервное копирование и восстановление файлов на уровне блоков вне хоста и мгновенное восстановление полной резервной копии VM для компьютеров-гостей Windows и Linux. Икрементные резервные копии не уровне блоков доступны, если компонент IBM Spectrum Protect for Virtual Environments используется вместе со средством перемещения данных IBM Spectrum Protect.

Кому предназначена эта публикация

Эта публикация предназначена для пользователей и администраторов, которые хотят установить и сконфигурировать IBM Spectrum Protect for Virtual Environments.

В публикации *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware: Руководство пользователя* представлена обзорная информация, задачи пользователей, сценарии резервного копирования и восстановления, справка по командам и сообщения об ошибках.

Публикации

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

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

Что нового в версии 8.1.7

В компоненте IBM Spectrum Protect for Virtual Environments версии 8.1.7 появились новые функции и обновления.

Список новых функций и обновлений в этом выпуске, а также в предыдущих выпусках версии 8 смотрите в разделе Обновления Data Protection for VMware.

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

Глава 1. Установка и обновление Data Protection for VMware

Установка компонента IBM Spectrum Protect for Virtual Environments включает в себя планирование, установку и первоначальное конфигурирование.

Устанавливаемые компоненты

Data Protection for VMware содержит несколько компонентов, которые можно установить для защиты виртуальной среды.

В зависимости от среды операционной системы для установки будут доступны следующие функции компонента Data Protection for VMware:

Ограничение: В каждом пакете установки есть файл лицензирования для пользователя (EULA). Если вы не примете этот файл, процесс установки остановится.

Таблица 1. Доступные функции Data Protection for VMware по операционным системам

Компонент	Linux	Windows
Агент восстановления IBM Spectrum Protect Этот компонент обеспечивает возможности виртуального монтирования и мгновенного восстановления.		√
Интерфейс командной строки агента восстановления Интерфейс командной строки, используемый для операций монтирования.		√
Документы Документы включают в себя файлы readme и файлы замечаний.	√	√
Файл полномочий Data Protection for VMware Этот компонент позволяет IBM Spectrum Protect выполнять следующие типы резервного копирования: • Резервное копирование Всегда инкрементное - Инкрементное • Резервное копирование Всегда инкрементное - Полное Этот компонент необходим для защиты приложений. Если вы выгружаете рабочие нагрузки резервного копирования, то этот файл нужно установить на сервере резервного копирования vStorage.	√	√

Таблица 1. Доступные функции Data Protection for VMware по операционным системам (продолжение)

Компонент	Linux	Windows
Графический интерфейс Data Protection for VMware vSphere Этот компонент является графическим пользовательским интерфейсом (graphical user interface, GUI), который получает доступ к данным VM на сервере VMware vCenter. Содержимое графического интерфейса доступно в следующих представлениях: • Представление веб-браузера. Доступ к этому представлению осуществляется в поддерживаемом веб-браузере с использованием URL хоста веб-сервера графического интерфейса. Например: `https://guihost.mycompany.com:9081/TsmVMwareUI/` • Представление компонента IBM Spectrum Protect vSphere Client - Модуль plugin на веб-клиента VMware vSphere. Панели в этом представлении специально предназначены для интеграции с веб-клиентом vSphere, но данные и команды для этого представления берутся с того же самого веб-сервера графического интерфейса, что и для других представлений. Компонент IBM Spectrum Protect vSphere Client - Модуль plugin обеспечивает подмножество функций, которые есть в представлении веб-браузера, и некоторые дополнительные функции. В этом представлении не предлагаются функции конфигурации и создания расширенных отчетов.	√	√
Графический интерфейс восстановления файлов Этот компонент представляет собой графический веб-интерфейс, который позволяет восстанавливать файлы из резервной копии виртуальной машины VMware без помощи администратора. Графический интерфейс устанавливается автоматически при установке графического интерфейса Data Protection for VMware. Он включается с помощью мастера конфигурации.	[1]	√
Узел перемещения данных Средство перемещения данных IBM Spectrum Protect перемещает данные для компонента Data Protection for VMware. Эту функцию называют средством перемещения данных. Средство перемещения данных перемещает данные из виртуальной среды на сервер IBM Spectrum Protect. При установке средства перемещения данных на сервере сервер можно использовать как сервер резервного копирования vStorage. Средство перемещения данных можно установить в той же системе, что и Data Protection for VMware, или на другом сервере.	√	√

1. Хотя компонент интерфейса восстановления файлов и следует устанавливать и включать в системах Windows, этот интерфейс можно использовать для восстановления файлов на виртуальных машинах-гостях как Windows, так и Linux.

2. При установке Data Protection for VMware средство перемещения данных включается в установку. В типичной установке не требуется дополнительное средство перемещения данных - оно будет установлено автоматически.

Data Protection for VMware выгружает нагрузку по резервному копированию с VM на сервер резервного копирования vStorage. Чтобы выполнить эту задачу, средство перемещения данных нужно установить на сервере резервного копирования vStorage.

Графический интерфейс Data Protection for VMware vSphere

Компонент Графический интерфейс Data Protection for VMware vSphere (графический интерфейс vSphere) - это графический пользовательский интерфейс (graphical user interface, GUI), который получает доступ к данным VM на сервере VMware vCenter.

Обзор

Графический интерфейс Data Protection for VMware vSphere - это первичный интерфейс, из которого можно выполнять следующие задачи:

- Инициировать или запланировать резервное копирование своих VM на сервере IBM Spectrum Protect.
- Инициировать полное восстановление своих VM с сервера IBM Spectrum Protect.
- Сгенерировать отчеты о ходе выполнения ваших задач, самых последних завершившихся событий, состоянии резервных копий и использовании пространства. Эта информация может помочь вам при устранении ошибок, связанных с резервным копированием.

Совет: Информация о том, как выполнить задачи с использованием графического интерфейса vSphere, представлена в электронной справке, устанавливаемой вместе с графическим интерфейсом. Щелкните по **Узнать подробнее** в любом из окон графического интерфейса, чтобы открыть электронную справку и получить помощь по задачам.

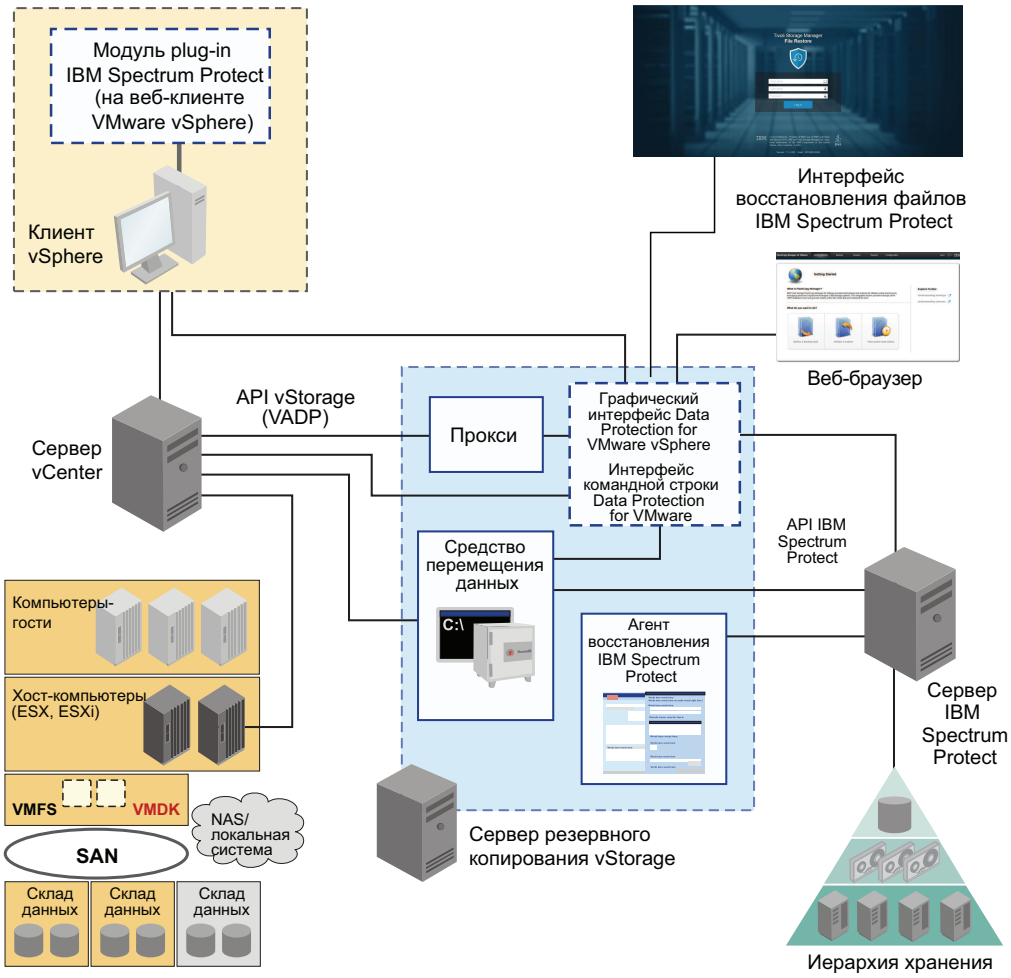

Рисунок 1. Компоненты системы Data Protection for VMware в среде пользователя vSphere VMware

Требования

Продукт Графический интерфейс Data Protection for VMware vSphere можно установить в любой системе, отвечающей требованиям к операционной системе. Требования к ресурсам графического интерфейса vSphere - минимальные, так как он не обрабатывает передачу данных ввода-вывода.

Совет: Установка графического интерфейса vSphere на сервере резервного копирования vStorage - это наиболее распространенная конфигурация.

У графического интерфейса vSphere должно быть сетевое соединение со следующими системами:

- Сервер резервного копирования vStorage
- Сервер IBM Spectrum Protect
- Сервер vCenter

Кроме того, должны быть доступны порты для базы данных Derby (по умолчанию `1527`) и веб-сервера графического интерфейса (по умолчанию `9081`).

Конфигурация

Можно зарегистрировать на одном сервере vCenter несколько графических интерфейсов vSphere. При таком сценарии сокращается число центров данных (и резервных копий их гостей VM), которыми управляет один графический интерфейс VMware vSphere. После этого сервер vCenter может управлять подмножеством из общего числа центров данных, заданных на сервере vCenter.

Чтобы обновить управляемые центры данных, выберите **Конфигурация > Изменить конфигурацию**.

При регистрации нескольких графических интерфейсов vSphere на одном сервере vCenter действуют следующие рекомендации:

- Каждый центр данных может управляться только одним установленным графическим интерфейсом vSphere.
- Для каждого установленного графического интерфейса vSphere требуется уникальное имя узла VMCLI.
- Использование уникальных имен узлов перемещения данных для каждого установленного графического интерфейса vSphere упрощает управление узлами.

Получение доступа к графическому интерфейсу vSphere

Доступ к графическому интерфейсу vSphere осуществляется следующими методами:

- Через графический интерфейс автономного веб-браузера. Доступ к этому графическому интерфейсу осуществляется через закладку URL на веб-сервере графического интерфейса, например:

  `https://`*`имя_хоста`*`:`*`порт`*`/TsmVMwareUI/`

  Здесь используются следующие обозначения:

  – *имя_хоста* - имя системы, где установлен Графический интерфейс Data Protection for VMware vSphere.

  – *порт* - номер порта, через который доступен графический интерфейс vSphere. Номер порта по умолчанию - 9080. Номер защищенного порта по умолчанию - 9081.

- Через расширение веб-клиента vSphere, которое соединяется с веб-сервером графического интерфейса для получения доступа к виртуальным машинам в хранилище IBM (оно называется расширением защиты данных). Содержимым является подмножество того, что представлено в графическом интерфейсе веб-браузера.

При установке можно задать один или несколько методов доступа.

Windows Каталог установки по умолчанию - `C:\IBM\SpectrumProtect\webserver`.

Linux Каталог установки по умолчанию - `/opt/tivoli/tsm/tdpvmware/common/webserver`.

Агент восстановления IBM Spectrum Protect

Используйте службу агента восстановления, чтобы смонтировать любой том снимка с сервера IBM Spectrum Protect.

Обзор

Для получения доступа к снимку из удаленной системы можно использовать протокол iSCSI.

Чтобы просмотреть снимок на локальном компьютере клиента с доступом 'только для чтения', используйте Data Protection for VMware версии 8.1.4 или более ранней.

Кроме того, агент восстановления обеспечивает как функцию мгновенного восстановления, так и защиту для приложений-гостей. Мгновенное восстановление позволяет используемому тому остаться доступным, когда операция восстановления продолжается в фоновом режиме. Защита приложений позволяет приложениям, установленным на виртуальной машине-госте, например, Microsoft Exchange Server и Microsoft SQL Server, быть доступными для защиты посредством резервного копирования и восстановления.

Агент восстановления может выполнить следующие задачи из удаленной системы:

- Собрать информацию о данных, которые можно восстановить, например:
  - Резервные копии VM.
  - Снимки, доступные для резервной копии виртуальной машины.
  - Разделы, доступные в конкретном снимке.

Подробную информацию о командах, параметрах и кодах возврата смотрите в разделе справочника по командам в публикации *IBM Spectrum Protect for Virtual Environments: Руководство пользователя Data Protection for VMware*.

Требования

Windows В Windows графический интерфейс агента восстановления и интерфейс командной строки устанавливаются как часть полной установки Data Protection for VMware или расширенной установки узла перемещения данных.

Доступ к агенту восстановления

Windows Доступ к агенту восстановления можно получить из меню **Пуск**: **Пуск > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > Агент восстановления IBM Spectrum Protect**

IBM Spectrum Protect vSphere Client - Модуль plugin

IBM Spectrum Protect vSphere Client - Модуль plugin - это расширение веб-клиента vSphere VMware, которое обеспечивает представление компонента Графический интерфейс Data Protection for VMware vSphere.

Обзор

В компоненте IBM Spectrum Protect vSphere Client - Модуль plugin есть подмножество функций, которые есть в представлении браузера для компонента Графический интерфейс Data Protection for VMware vSphere, и некоторые дополнительные функции.

Требование

Чтобы установить компонент IBM Spectrum Protect vSphere Client - Модуль plugin, нужно при запуске мастера конфигурирования IBM Spectrum Protect for Virtual Environments выбрать следующие опции:

- На странице **Параметры vCenter** в мастере конфигурирования выберите **Обновить регистрацию**, чтобы зарегистрировать модуль plug-in в связанном компоненте vCenter.
- Введите адрес хоста графического интерфейса, укажите пользователя vCenter и пароль.

  Примечание: Домен по умолчанию основан на локальном адресе домена и может не быть доступен извне. Если требуется внешний доступ, укажите адрес хоста графического интерфейса, который можно разрешить с помощью DNS или IP-адреса.

По завершении работы с мастером модуль plug-in будет зарегистрирован в vCenter.

Получение доступа к модулю plugin защиты данных

Доступ к этому модулю plugin можно получить из веб-клиента vSphere:

1. Войдите в веб-клиент vSphere с идентификационными данными vCenter. Модуль plugin защиты данных находится в главном меню - **IBM Spectrum Protect**.
2. Если вы выберете этот пункт меню, то вы перейдете в главную область расширения IBM Spectrum Protect. В разделах **Мониторинг** и **Конфигурирование**, связанных с конкретным элементом в перечне vCenter, будет также функция IBM Spectrum Protect for Virtual Environments.

интерфейс командной строки Data Protection for VMware

интерфейс командной строки Data Protection for VMware - это полнофункциональный интерфейс командной строки, установленный вместе с компонентом Графический интерфейс Data Protection for VMware vSphere.

Обзор

интерфейс командной строки Data Protection for VMware можно использовать для выполнения следующих задач:

- Инициировать или запланировать резервное копирование своих VM на сервере IBM Spectrum Protect.
- Инициировать полное восстановление своих VM, файлов VM или дисков VM (VMDK) с сервера IBM Spectrum Protect.
- Просмотреть информацию о конфигурации для базы данных и среды резервного копирования.

Хотя Графический интерфейс Data Protection for VMware vSphere - это основной интерфейс задач, интерфейс командной строки Data Protection for VMware обеспечивает полезный вторичный интерфейс.

Например, интерфейс командной строки Data Protection for VMware можно использовать для реализации механизма планирования, отличающегося от механизма, реализованного компонентом Графический интерфейс Data Protection for VMware vSphere. Кроме того, интерфейс командной строки Data Protection for VMware полезен при оценке результатов автоматизации с помощью сценариев.

Получение доступа к компоненту интерфейс командной строки Data Protection for VMware

Получить доступ к компоненту интерфейс командной строки Data Protection for VMware можно из командной строки.

Подробную информацию о доступных командах смотрите в разделе справочника по командам в публикации *IBM Spectrum Protect for Virtual Environments: Руководство пользователя Data Protection for VMware*.

Интерфейс восстановления файлов IBM Spectrum Protect

Отдельные файлы можно восстанавливать из резервной копии виртуальной машины VMware.

Обзор

Интерфейс восстановления файлов - это веб-интерфейс, в котором можно восстанавливать отдельные файлы из резервной копии VM. Преимуществом этого интерфейса является то, что владельцы файлов, программ и платформ могут восстановить свои собственные файлы, ничего заранее не зная об операциях резервного копирования и восстановления IBM Spectrum Protect.

Компонент интерфейса восстановления файлов устанавливается, когда вы выбираете опцию защиты ваших данных в среде vSphere. В мастере конфигурирования компонента Data Protection for VMware нужно включить функцию восстановления файлов, чтобы этот интерфейс стал доступен.

Получение доступа к интерфейсу восстановления файлов IBM Spectrum Protect

Чтобы получить доступ к интерфейсу восстановления файлов, откройте веб-браузер и введите URL, который вам сообщил ваш администратор. Например:

`https://`*`hostname`*`:9081/FileRestoreUI`

где *имя_хоста* - это имя хоста системы, в которой установлен Графический интерфейс Data Protection for VMware vSphere.

Функция перемещения данных

Функция перемещения данных - это программный компонент Data Protection for VMware, который перемещает данные в компонент Сервер IBM Spectrum Protect и из него.

Обзор

В типичной среде VMware средство перемещения данных используется для сохранения резервных копий виртуальной машины на узле центра данных.

При установке Data Protection for VMware функция перемещения данных включается в установку. Функция перемещения данных устанавливается в той же системе, где находится компонент Графический интерфейс Data Protection for VMware vSphere и другие компоненты Data Protection for VMware.

Также можно установить функции перемещения данных в удаленных системах независимо от других компонентов Data Protection for VMware, чтобы перераспределить рабочую нагрузку по резервному копированию по нескольким системам.

Операции дифференциального резервного копирования снимков не поддерживаются в среде VMware. Запустить операции дифференциального резервного копирования снимков файловой системы, находящейся на файл-сервере NetApp на хосте, где также установлена функция перемещения данных Data Protection for VMware, нельзя.

Настройка средств перемещения данных

Информацию о планировании, установке и конфигурировании средств перемещения данных смотрите в следующем списке:

Действие	**Описание**
Определите число функций перемещения данных, которых потребуются, чтобы защитить вашу среду vSphere.	Для защиты среды vSphere может потребоваться несколько функций перемещения данных. Чтобы определить число необходимых узлов перемещения данных, смотрите техническое замечание 2007197. Это техническое замечание также содержит обсуждение использования виртуальных машин или физических компьютеров для узлов перемещения данных и для размещения функции перемещения данных.
Установите Data Protection for VMware.	Чтобы установить Data Protection for VMware, запустите программу установки Data Protection for VMware и выберите **Стандартная установка** в операционных системах Windows либо **Полная** - в операционных системах Linux. Эта опция установки позволяет установить все компоненты Data Protection for VMware, включая средство перемещения данных. Информацию об использовании установщика Data Protection for VMware смотрите в разделе “Установка компонентов Data Protection for VMware” на стр. 24.

Действие	Описание
Задайте средства перемещения данных для вашей среды.	Когда мастер установки Data Protection for VMware завершит работу, откроется мастер конфигурирования компонента Графический интерфейс Data Protection for VMware vSphere, чтобы вы смогли настроить взаимодействия с компонентом Сервер IBM Spectrum Protect. На странице Узлы перемещения данных в мастере конфигурирования задайте информацию для локальной функции перемещения данных и для всех удаленных функций перемещения данных, которые вы установите в отдельных системах. Если вы производите установку в операционной системе Windows и выбираете **Создать службы**, когда задаете функцию перемещения данных, информация о конфигурации функции перемещения данных сохраняется в файле опций в следующем расположении: `C:\Program Files\Tivoli\TSM\baclient\` Кроме того, конфигурируются службы, которые требуются для функции перемещения данных. Если вы установите функцию перемещения данных в операционной системе Linux или в операционной системе Windows, не выбирая опцию **Создать службы** при конфигурировании, вы должны будете выполнить шаги в разделе “Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere” на стр. 97, чтобы создать файл опций и сконфигурировать необходимые службы.
Установите и сконфигурируйте дополнительные функция перемещения данных в удаленных системах. если потребуется.	Чтобы установить средство перемещения данных в удаленной системе, запустите программу установки Data Protection for VMware и выполните одно из следующих действий: В операционных системах Windows выберите в мастере конфигурирования **Расширенная установка > Установить только функцию перемещения данных**. В операционных системах Linux выберите в мастере конфигурирования **Пользовательская** в списке **Набор установки**. Убедитесь, что выбрана опция **Узел перемещения данных Data Protection for VMware**. Эта опция выбрана по умолчанию. По завершении установки выполните инструкции в разделе “Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere” на стр. 97, чтобы настроить функции перемещения данных в удаленных системах.

Планирование установки Data Protection for VMware

Data Protection for VMware устраняет влияние выполнения резервного копирования на VM, выгружая рабочую нагрузку с хоста на основе VMware ESXi на сервер резервного копирования vStorage.

Data Protection for VMware работает со встроенным средством перемещения данных для выполнения полного резервного копирования Всегда инкрементное и инкрементного резервного копирования Всегда инкрементное VM. Узел перемещения данных "перемещает" данные на сервер IBM Spectrum Protect для хранения и для последующего восстановления на уровне образа VM. Мгновенное восстановление доступно на уровне дискового тома и на уровне полной VM.

Совет: Средство перемещения данных - это отдельно лицензируемый компонент, содержащим свои собственные пользовательские интерфейсы и документацию. Знакомство с этим продуктом и с документацией к нему необходимо, чтобы правильно интегрировать полный план защиты виртуальных машин с Data Protection for VMware. Data Protection for VMware для 64-разрядной системы Windows содержит функцию перемещения данных.

Дорожная карта установки

В следующей таблице указано, какие шаги нужно выполнить для успешного завершения процесса установки.

Таблица 2. Задачи по установке для новых или существующих заказчиков Data Protection for VMware

Шаг	Задача	Начните здесь
1	Проверить требования к системе.	Убедитесь система, в которой будет установлен продукт Data Protection for VMware, соответствует требованиям к системе.
2	Проверить требования к разрешениям пользователей.	Избегайте потенциальных ошибок установки или задержек, используя нужные уровни разрешений пользователей.
3	Проверяйте доступность нужных портов связи.	Предотвращайте ошибки или задержки установки, открывая нужные порты связи до попытки установить компонент Data Protection for VMware.
4	Установите Data Protection for VMware: • Установка Data Protection for VMware при помощи мастера установки • “Установка компонентов Data Protection for VMware в режиме без вывода сообщений” на стр. 29 Обновите Data Protection for VMware: Обновить Data Protection for VMware	В каждом пакете установки есть файл лицензирования для пользователя (EULA). Если вы не принимаете этот файл, то установка прекращается.

Таблица 2. Задачи по установке для новых или существующих заказчиков Data Protection for VMware (продолжение)

Шаг	Задача	Начните здесь
5	"Конфигурирование новой установки при помощи мастера" на стр. 45 Если вы собираетесь обновить Data Protection for VMware в зависимости от установленных компонентов, может потребоваться больше задач по конфигурированию. Смотрите разделы по конфигурации в публикации *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware: Руководство пользователя*, чтобы узнать об этом подробнее.	Используйте мастер конфигурирования для первоначального конфигурирования. В зависимости от установленных функций может потребоваться больше задач по конфигурированию, чем описано в этом разделе.

Совет: Чтобы помочь спланировать количество прокси-хостов, необходимых для конкретной среды резервного копирования компонента Data Protection for VMware, в википедии IBM Spectrum Protect есть следующая публикация:
Пошаговое руководство по определению размера сервера резервного копирования (прокси) vStorage
Эта публикация доступна в разделе продукта IBM Spectrum Protect for Virtual Environments.

Сценарии установки

Перед установкой Data Protection for VMware выберите сценарий, который лучше всего отвечает вашим бизнес-потребностям.

Data Protection for VMware и средство перемещения данных можно установить с использованием графического интерфейса или режима без вывода сообщений:

- "Установка компонентов Data Protection for VMware при помощи мастера установки" на стр. 26
- "Установка компонентов Data Protection for VMware в режиме без вывода сообщений" на стр. 29

Список функций и компонентов, доступных для платформы, смотрите в разделе "Устанавливаемые компоненты" на стр. 1.

Таблица 3. Сценарии установки

Номер сценария	Описание	Задачи, которые нужно выполнить
1	Используйте этот сценарий для новой установки, когда вы хотите установить Data Protection for VMware и средство перемещения данных в одной и той же системе.	Windows Можно использовать программу установки комплекта (Suite Installer) в режиме графического интерфейса или в режиме без вывода сообщений. Linux Можно использовать InstallAnywhere в режиме графического интерфейса или в режиме без вывода сообщений.

Таблица 3. Сценарии установки (продолжение)

Номер сценария	Описание	Задачи, которые нужно выполнить
2	Используйте этот сценарий, если вы хотите установить средство перемещения данных (прокси-сервер монтирования), агент восстановления и необходимые пакеты поддержки в этой системе.	Windows Можно выполнить расширенную установку, используя программу установки коммплекта. Linux Теперь средство перемещения данных устанавливается вместе с компонентом Data Protection for VMware.

Требования к системе

Чтобы реализовать компоненты Data Protection for VMware, система должна удовлетворять соответствующим требованиям к системе.

Требования к программному обеспечению

Сведения о требованиях к программному обеспечению и к операционной системе могут изменяться со временем. Текущие требования к программному обеспечению смотрите в technote 1505139.

Требования к аппаратным средствам

Требования к аппаратному обеспечению зависят от следующих параметров:

- Число защищенных серверов
- Число защищенных томов
- Размеры наборов данных
- Возможности соединений в локальной сети и в сети SAN

Примечание: агент восстановления не поддерживает операции в среде без использования локальной сети/

В следующей таблице описаны требования к аппаратному обеспечению для установки Data Protection for VMware.

Таблица 4. Требования к аппаратному обеспечению для Data Protection for VMware.

Компонент	Минимальные требования	Предпочтительно
Система	Процессор IntelPentium D Dual Core или совместимый с ним.	Неприменимо
Память	4 ГБ оперативной памяти, 4 ГБ виртуального адресного пространства	Неприменимо
Свободное место на жестком диске	4.4 ГБ	9.0 ГБ
Сеть	1 GbE	10 GbE

Примечание: В зависимости от числа параллельных процессов для резервного копирования виртуальных машин потребуется значительный объем памяти.

Требования к памяти можно увеличить по отношению к команде **dsmc backup vm**; их можно вычислить по следующей формуле:

Необходимая память = (DiskSize / MBLKSize) * ReadBufferSize * VMMAXPARALLEL

Здесь используются следующие обозначения:

- **DiskSize** - это размер гостевого диска, который сейчас обрабатывается;
- **MBLKSize** - это размер мегаблока. Он равен 128 МБ для дисков, объемом менее 2 ТБ, и равен 1 ГБ для дисков, объемом более 2 ТБ.
- **ReadBufferSize** - это размер внутреннего буфера IBM Spectrum Protect, использующегося для соответствия информации MBLK. Размер буфера равен 256 КБ.
- **VMMAXPARALLEL** - это максимальное число виртуальных машин, резервное копирование которых можно выполнить одновременно в любой момент с использованием одного процесса резервного копирования.

Например, чтобы создать резервные копии 10 гостей, на каждом из которых есть диски по 40 ГБ и которые работают в режиме VMMAXPARALLEL 2 с одним процессом операции резервного копирования, потребуется:

- **DiskSize** = 40 ГБ = 41943040 КБ;
- **MBLKSize** = 128 МБ = 131072 КБ;
- **ReadBufferSize** = 256 КБ;
- **VMMAXPARALLEL** = 2.

Необходимая память = (41943040 / 131072) * 256 КБ * 2 = 163840 КБ = 160 МБ.

Примечание: Чтобы создать резервные копии того же числа гостей с 'VMMAXPARALLEL 2' в пяти параллельных процессах операции резервного копирования, потребовалось бы (максимум) в пять раз больше памяти, чем в предыдущем примере, то есть, 800 МБ.

Ограничение: В отношении VMDK VMware, задействованных в операции резервного копирования, применяются следующие ограничения:

- В режиме инкрементного резервного копирования Всегда инкрементное каждый отдельный VMDK, участвующий в операции резервного копирования, не должен содержать более 8 ТБ. Если VMDK превышает 8 ТБ, операция резервного копирования завершится неудачно. Чтобы увеличить размер VMDK до размера, превышающего 2 ТБ по умолчанию, задайте максимальный размер с помощью опции `vmmaxvirtualdisks`. Чтобы получить дополнительную информацию, ищите `vmmaxvirtualdisks` в IBM Knowledge Center.
- В режиме полного резервного копирования Всегда инкрементное каждый отдельный VMDK, участвующий в операции резервного копирования, не должен содержать более 2 ТБ. Если VMDK превышает 2 ТБ, операция резервного копирования завершится неудачно.

Чтобы не допустить ошибки при работе в любом режиме резервного копирования, можно пропустить обработку VMDK, задав `vmskipmaxvirtualdisks yes` в файле опций перемещения данных. Дополнительные сведения смотрите в разделе Vmskipmaxvirtualdisks.

Требования к восстановлению файлов

Перед восстановлением файлов использованием интерфейса восстановления файлов IBM Spectrum Protect Data Protection for VMware убедитесь, что ваша среда соответствует минимальным требованиям.

Чтобы включить функцию восстановления файлов, продукт Data Protection for VMware должен быть установлен в системе Windows.

Требования к виртуальным машинам VMware

Приведенные ниже требования касаются виртуальных машин VMware, которые содержат файлы, подлежащие восстановлению:

- Linux Windows На виртуальной машине должен быть установлен инструмент VMware Tools.
- Linux Windows Виртуальная машина во время операции восстановления файлов должна работать.
- Windows Система перемещения данных должна либо принадлежать к тому же домену Windows, либо находиться в домене с доверенными отношениями с виртуальной машиной на которой содержатся восстанавливаемые файлы.
- Windows При удалении виртуальной машины из домена Windows и ее последующем восстановлении виртуальная машина должна заново объединиться с доменом, чтобы гарантировать взаимосвязь доверительных отношений с доменом. Не пытайтесь восстанавливать файлы с виртуальной машины, пока не будет восстановлена взаимосвязь доверия с доменом.
- Windows Если пользователь не является владельцем файла, который нужно восстановить, полномочие Microsoft Windows `Восстановление файлов и каталогов` нужно назначить пользователю этой виртуальной машины.
- Дальнейшую информацию о предварительных требованиях к учетной записи домена Microsoft Windows для использования интерфейса восстановления файлов Data Protection for VMware смотрите в техническом замечании 1998066.
- Linux Для виртуальной машины требуется локальная аутентификация пользователя. Аутентификация через домен Windows, Lightweight Directory Access Protocol (LDAP), Kerberos или другие методы сетевой аутентификации, недоступна.
- Linux В операционной системе Red Hat Enterprise Linux 6 опция `ChallengeResponseAuthentication` в файле конфигурации демона sshd (`/etc/ssh/sshd_config`) должна задавать значение YES или должна быть закомментирована. Например, действительным является любой из следующих операторов:

  ```
  ChallengeResponseAuthentication yes
  #ChallengeResponseAuthentication no
  ```

  После изменения этой опции перезапустите демон sshd.

Необходимые условия перемещения данных

Система перемещения данных соответствует определенному средству перемещения данных, которые "перемещают данные" из одной системы в другую.

Windows Система перемещения данных должна принадлежать к тому же домену Windows, что и виртуальная машина, на которой содержатся файлы, подлежащие восстановлению.

Требования к прокси монтирования

Система прокси монтирования представляет собой систему прокси Linux или Windows, которая получает доступ к смонтированным дискам виртуальной машины через соединение iSCSI. Эта система позволяет сделать файловые системы на смонтированных дисках виртуальных машин доступными в виде точек монтирования в интерфейсе восстановления файлов.

Linux В операционной системе Linux есть демон, который активирует группу томов менеджера логических томов (Logical Volume Manager, LVM), когда эти группы становятся доступны системе. Настройте этот демон в системе прокси монтирования Linux, так чтобы эти группы томов LVM не активировались, когда они становятся доступны системе. Подробную информацию о том, как настроить этот демон, смотрите в соответствующей документации Linux.

Linux Windows Система прокси монтирования Windows и система прокси монтирования Linux должны находиться в одной и той же подсети.

Требования к учетной записи домена Microsoft Windows

Следующие необходимые условия работы относятся учетным записям домена Windows. Первое требование - задать учетную запись пользователя домена Windows с локальными административными полномочиями на всех виртуальных машинах:

- Чтобы выполнить необходимые задачи для включения восстановления файлов на гостевой виртуальной машине, вам нужна учетная запись пользователя, которая принадлежит домену Windows и является локальным администратором на монтируемой прокси-системе. Администратор с этой учетной записью вводит идентификационные данные в мастере по конфигурированию графического пользовательского интерфейса Data Protection for VMware vSphere или в блокноте, чтобы разрешить для среды операции восстановления файлов.
- Чтобы создать учетную запись пользователя с необходимыми привилегиями для использования интерфейса восстановления файлов, можно использовать объект групповой политики Windows для централизованного управления одним пользователем домена, что позволит ему обращаться к нескольким машинам с идентификационными данными локального администратора, и дополнительно ограничивать нежелательные действия.

Следующие действия показывают, как можно создать эту учетную запись пользователя. Выполните эти действия на контроллере домена при помощи оснастки Active Directory Users и Computers MMC:

1. Выберите **Действие->Создать->Группы** и создайте новую группу безопасности с именем **FR Admins**. Область действия группы должна быть задана как `Глобальная`.
2. Создайте новую учётную запись пользователя домена с именем пользователя `fradmin1` и добавьте ее в группу защиты **FR Admins**. Можно также добавить в эту группу другие учётные записи пользователей домена.
3. Чтобы обеспечить дополнительный контроль над набором компьютеров, к которым может обращаться `fradmin1`, создайте новую организационную единицу
4. Из объекта домена выберите **Создать->Организационная единица** и назовите ее `FR Computers`
5. Включите компьютеры в организационную единицу `FR Computers` .

Выполните следующие действия на контроллере домена из оснастки Group Policy MMC:

1. Создайте новый объект групповой политики с именем `FR Admin GPO`, который добавит администраторов группы **FR Admins** в группу локальных администраторов компьютеров, связанных с организационной единицей, к которой применяется этот объект групповой политики.
2. В объекте групповой политики добавьте учётную запись и в группу локальных администраторов и, если требуется, в группу пользователей удаленного рабочего стола.
3. Выберите организационную единицу `FR Computers` и добавьте только что созданный объект групповой политики.

   Примечание: Объект групповой политики можно связать с самим доменом, но тогда `fradmin1` будет в группе локальных администраторов для всех компьютеров в домене. Использование явной организационной единица дает дополнительный контроль.
4. Необязательно: используйте управление групповыми политиками, чтобы ограничить нежелательные действия на локальном компьютере, например, задать `Запрещение локального входа в систему` и `Запрещение входа в систему через Terminal Services`.
5. На странице Восстановление файлов мастера по конфигурированию пользовательского графического интерфейса Data Protection for VMware vSphere или в блокноте измените параметры, чтобы использовать созданную на предыдущих шагах учетную запись `domain\fradmin1`.
6. Перезапустите службу монтирования прокси демона доступа клиентов (client access daemon, CAD).

Когда вы задали учётную запись с подходящими привилегиями:

- Windows Введите свои учетные данные в мастере конфигурации или блокноте компонента Графический интерфейс Data Protection for VMware vSphere, чтобы включить в среде операции восстановления файлов.
- Windows Владелец файлов получает доступ к удаленной виртуальной машине (где содержатся файлы, которые нужно восстановить), используя идентификационные данные пользователя домена Windows. Эти идентификационные данные вводятся в интерфейс восстановления файлов при входе в систему. Идентификационные данные пользователя домена позволяют проверить, есть ли у владельца файла разрешение на вход в систему удаленной виртуальной машины и на восстановление файлов на удаленной виртуальной машине. Для этих идентификационных данных не требуется никаких специальных полномочий.
- Windows Если владелец файла использует учетную запись пользователя домена Windows, для которой ограничен доступ к тем или иным компьютерам (вместо доступа ко всем компьютерам в домене), убедитесь, что система прокси монтирования включена в список компьютеров, которые доступны для этой учетной записи пользователя домена. В противном случае владелец файла не сможет войти в интерфейс восстановления файлов.

Необходимые условия для ленточных устройств

Восстановление файлов с ленточного носителя не поддерживается. Восстановление файлов из дискового хранилища является предпочтительным методом.

Необходимые разрешения на установку

Прежде чем приступать к установке, убедитесь, что у вашего ID пользователя есть необходимый уровень разрешений.

Об этой задаче

Таблица 5. Разрешения пользователя, необходимые для установки и конфигурирования компонента Data Protection for VMware

Система	Необходимое разрешение
Windows	Администратор
Linux	Root
Сервер vCenter	Полномочия администратора Роли сервера vCenter требуются следующие полномочия: **Расширение > Зарегистрировать расширение, Дерегистрировать расширение, Обновить расширение**. Эту новую роль нужно применить к объекту vCenter в иерархии сервера VMware vCenter для ID пользователя, указанного при установке.
Сервер IBM Spectrum Protect **Ограничение:** Сервер должен быть запущен.	Доступ администратора (Полномочия **Система** или **Неограниченный домен политики**)

Необходимые порты связи

Смотрите список портов связи, которые должны быть открыты на брандмауэре при установке компонента Data Protection for VMware.

Порты, указанные в таблице, отражают стандартную установку. Стандартная установка состоит из следующих компонентов в одной и той же системе Windows:

- Сервер графического интерфейса Data Protection for VMware
- сервер резервного копирования vStorage (средство перемещения данных)
- Прокси монтирования Windows
- Интерфейс восстановления файлов IBM Spectrum Protect

Если используется нестандартная установка, может потребоваться больше портов.

Ограничение: Прокси монтирования Windows и прокси монтирования Linux должны быть в одной и той же подсети.

Таблица 6. Необходимые порты связи. В этой таблице указаны порты, доступ к которым получает компонент Data Protection for VMware.

Порт TCP	Инициатор: Исходящий (с хоста)	Назначение: Входящий (на хост)
443	Сервер резервного копирования vStorage	Сервер vCenter (защищенный HTTP)
443	Сервер Графический интерфейс Data Protection for VMware vSphere	Сервер vCenter

Таблица 6. Необходимые порты связи (продолжение). В этой таблице указаны порты, доступ к которым получает компонент Data Protection for VMware.

Порт TCP	Инициатор: Исходящий (с хоста)	Назначение: Входящий (на хост)
443 Этот параметр требуется, только если средство перемещения данных представляет собой систему Linux.	Прокси монтирования Windows	Сервер vCenter
443	Сервер резервного копирования vStorage	Контроллер служб платформы
443	Сервер Графический интерфейс Data Protection for VMware vSphere	Контроллер служб платформы
443	Прокси монтирования Windows	Контроллер служб платформы
902 443	Сервер vCenter	Хосты ESXi
902 443	Сервер резервного копирования vStorage (прокси)	Хосты ESXi (все защищенные хосты)
1500 (**tcpport**)	Сервер резервного копирования vStorage (прокси)	Сервер IBM Spectrum Protect
1500 (**tcpadminport**)	Сервер Графический интерфейс Data Protection for VMware vSphere • Порт 1500 (**порт_администрирования_tcp**) относится к связи не SSL • Для связи SSL **порт_администрирования_tcp** - это единственный порт, поддерживающий связь SSL с сервером IBM Spectrum Protect. Правильный номер порта, который нужно использовать для протокола SSL, это, обычно, значение, заданное опцией **ssltcpadminport** в файле dsmserv.opt сервера IBM Spectrum Protect. Однако, если в файле dsmserv.opt задана опция **adminonclient no**, правильным номером порта, который следует использовать для протокола SSL, будет значение, заданное опцией **ssltcpadminport**. У опции **ssltcpadminport** нет значения по умолчанию. Поэтому значение должен задать пользователь.	Сервер IBM Spectrum Protect
1527 Внутренняя база данных Derby		

Таблица 6. Необходимые порты связи (продолжение). В этой таблице указаны порты, доступ к которым получает компонент Data Protection for VMware.

Порт TCP	Инициатор: Исходящий (с хоста)	Назначение: Входящий (на хост)
1501 1581 (**httpport**)	Сервер IBM Spectrum Protect	Сервер резервного копирования vStorage • Планировщик перемещения данных • Веб-клиент • Демон Client Acceptor
1581 (**httpport**) 1582, 1583 (**webports**)	Сервер Графический интерфейс Data Protection for VMware vSphere	Сервер резервного копирования vStorage
9081 Веб-сервер графического интерфейса (протокол HTTPS)	Клиент vSphere	Сервер Графический интерфейс Data Protection for VMware vSphere (защищенный порт HTTPS для доступа к vCenter через веб-браузер)
22 Порт SSH по умолчанию для агента восстановления	Агент восстановления	Хост монтирования Data Protection for VMware Windows • SSH для агента восстановления Linux
3260	Восстановление файлов Data Protection for VMware в Linux	Хост монтирования Data Protection for VMware Windows • iSCSI
3260 Порт iSCSI по умолчанию для агента восстановления	Объект назначения Windows с динамическим диском для восстановления файлов	Хост монтирования Data Protection for VMware Windows • iSCSI
5985	Опции графического интерфейса по восстановлению файлов	Удаленное управление Windows
135	Прокси монтирования Windows	Виртуальная машина VMware, которая содержит файлы, подлежащие восстановлению интерфейсом восстановления файлов IBM Spectrum Protect

Требования к полномочиям пользователя сервера VMware vCenter

Для выполнения операций Data Protection for VMware требуются некоторые особые полномочия сервера VMware vCenter.

Полномочия сервера vCenter, необходимые для защиты центров данных VMware с представлением веб-браузера для Графический интерфейс Data Protection for VMware vSphere

У ID пользователя сервера vCenter, который входит в представление браузера для Графический интерфейс Data Protection for VMware vSphere,

должны быть достаточные полномочия VMware, чтобы просматривать содержимое центра данных, управляемого графическим интерфейсом.

Например, среда VMware vSphere содержит пять центров данных. У пользователя “jenn” достаточно полномочий только для двух из этих центров данных. Поэтому в представлениях пользователь “jenn” увидит только два из этих центров данных, для доступа к которым у него есть достаточные полномочия. Другие три центра данных (на доступ к которым у пользователя “jenn” нет полномочий) будут не видны пользователю “jenn”.

Сервер VMware vCenter задает ряд полномочий в совокупности в виде роли. Роль применяется к объекту для указанного пользователя или группы, чтобы создать полномочия. Вы должны создать роль с набором полномочий с веб-клиента VMware vSphere. Чтобы создать роль сервера vCenter для операций резервного копирования и восстановления, используйте функцию **Добавить роль** на клиенте VMware vSphere.

Если вы хотите распространить эти полномочия на все центры данных в пределах vCenter, задайте сервер vCenter и включите переключатель `распространять на дочерние`. Или вы можете ограничить разрешения, если назначите роль для нужных центров данных, только при включенном переключателе `распространять на дочерние`. Принудительное применение для графического интерфейса браузера находится на уровне центра данных.

В следующем примере показано, как управлять доступом к центрам данных для двух групп пользователей VMware. Сначала создайте роль, у которой будут все полномочия, указанные в technote 7047438. Набор полномочий в этом примере указан ролью “TDPVMwareManage”. Группе 1 требуется доступ, чтобы управлять виртуальными машинами для центров данных `Primary1_DC` и `Primary2_DC`. Группе 2 требуется доступ, чтобы управлять виртуальными машинами для центров данных `Secondary1_DC` и `Secondary2_DC`.

Назначьте группе 1 роль “TDPVMwareManage” для центров данных `Primary1_DC` и `Primary2_DC`. Назначьте группе 2 роль “TDPVMwareManage” для центров данных `Secondary1_DC` и `Secondary2_DC`.

Пользователи в каждой группе пользователей VMware смогут использовать графический интерфейс Data Protection for VMware для управления виртуальными машинами только в соответствующих центрах данных.

Совет: При создании роли рассмотрите возможность добавить в роль дополнительные полномочия, которые могут потом понадобиться для выполнения других задач с объектами.

Полномочия сервера vCenter, необходимые для использования средства перемещения данных

Средству перемещения данных IBM Spectrum Protect, установленное на сервере резервного копирования vStorage Backup (узел перемещения данных), требуются опции `VMCUser` и `VMCPw`. Опция `VMCUser` задает ID пользователя сервера vCenter или ESX, который вам нужен, чтобы производить резервное копирование, восстановление или запрос. Необходимые полномочия, назначенные этому ID пользователя (`VMCUser`), гарантируют, что клиент сможет выполнять операции на виртуальной машине и в среде VMware. У этого ID пользователя должны быть полномочия VMware, описанные в указанной выше технической записке.

Чтобы создать роль сервера vCenter для операций резервного копирования и восстановления, используйте функцию **Добавить роль** на клиенте VMware vSphere. При добавлении полномочий для этого ID пользователя (`VMCUser`) вы должны выбрать опцию `распространять на дочерние`. Кроме того, рассмотрите возможность добавления в эту роль других полномочий для задач помимо резервного копирования и восстановления. Для опции `VMCUser` принудительное применение осуществляется для объекта высшего уровня.

Полномочия сервера vCenter, необходимые для защиты центров данных VMware с представлением IBM Spectrum Protect vSphere Client - Модуль plugin для Графический интерфейс Data Protection for VMware vSphere

Компоненту IBM Spectrum Protect vSphere Client - Модуль plugin требуется набор полномочий отдельно от полномочий, необходимых для входа в графический интерфейс.

При установке для компонента IBM Spectrum Protect vSphere Client - Модуль plugin создаются следующие пользовательские полномочия:

- **Центр данных > IBM Data Protection**
- **Глобальные > Сконфигурировать IBM Data Protection**

Пользовательские полномочия, которые необходимы для компонента IBM Spectrum Protect vSphere Client - Модуль plugin, регистрируются как отдельное расширение. Ключ расширения полномочий - `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Эти полномочия позволяют администратору VMware включать и выключать доступ к содержимому компонента IBM Spectrum Protect vSphere Client - Модуль plugin. Получать доступ к содержимому IBM Spectrum Protect vSphere Client - Модуль plugin могут только пользователи с этими пользовательскими полномочиями для необходимого объекта VMware. Для каждого сервера vCenter регистрируется по одному компоненту IBM Spectrum Protect vSphere Client - Модуль plugin, и он совместно используется всеми хостами графического интерфейса, сконфигурированными для поддержки сервера vCenter.

На веб-клиенте VMware vSphere нужно создать роль для пользователей, которые смогут выполнять функции защиты данных для виртуальных машин, используя компонент IBM Spectrum Protect vSphere Client - Модуль plugin. Для этой роли, в дополнение к стандартным полномочиям роли администратора виртуальных машин, необходимым веб-клиенту, нужно задать полномочия **Центр данных > IBM Data Protection**. Для каждого центра данных назначьте эту роль каждому пользователю

или группе пользователей, пользователям которой вы хотите предоставить разрешение на управление виртуальными машинами.

Полномочия **Глобальный > IBM Data Protection** необходимы пользователю на уровне vCenter. Это полномочие позволяет пользователю управлять, изменять или стирать соединение между сервером vCenter и веб-сервером Графический интерфейс Data Protection for VMware vSphere. Назначьте эти полномочия администраторам, которые знакомы с компонентом Графический интерфейс Data Protection for VMware vSphere, который защищает соответствующий сервер vCenter. Управляйте соединениями компонента IBM Spectrum Protect vSphere Client - Модуль plugin на странице Соединения расширения.

В следующем примере показано, как управлять доступом к центрам данных для двух групп пользователей. Группе 1 требуется доступ, чтобы управлять виртуальными машинами для центров данных `NewYork _DC` и `Boston_DC`. Группе 2 требуется доступ, чтобы управлять виртуальными машинами для центров данных `LosAngeles_DC` и `SanFranciso_DC`.

На клиенте VMware vSphere создайте, например, роль “IBMDataProtectManage”, назначьте стандартные полномочия роли администратора виртуальных машин, а также полномочия **Центр данных > IBM Data Protection**.

Назначьте группе 1 роль “IBMDataProtectManage” для центров данных `NewYork_DC` и `Boston_DC`. Назначьте группе 2 роль “IBMDataProtectManage” для центров данных `LosAngeles_DC` и `SanFranciso_DC`.

Пользователи в каждой группе смогут использовать компонент IBM Spectrum Protect vSphere Client - Модуль plugin на веб-клиенте vSphere для управления виртуальными машинами только в соответствующих центрах данных.

Проблемы, связанные с недостаточными полномочиями

Если у пользователя веб-браузера нет достаточных полномочий ни для какого центра обработки данных, доступ к представлению блокируется. Вместо этого генерируется сообщение об ошибке GVM2013E, чтобы указать, что пользователь не авторизован для получения доступа ни к каким управляемым центрам данных из-за недостатка разрешений. Также есть другие новые сообщения, которые информируют пользователей о проблемах из-за недостаточных разрешений. Чтобы устранить проблемы, связанные с разрешениями, убедитесь, что роль пользователя задана, как рассказывается в предыдущих разделах. У роли пользователя должны быть все полномочия, указанные в необходимых полномочиях для ID пользователя сервера vCenter и таблицы перемещения данных, и эти полномочия должны быть применены на уровне центра данных с включенным переключателем `распространять на дочерние`.

Если у пользователя компонента IBM Spectrum Protect vSphere Client - Модуль plugin нет достаточных полномочий на доступ к центру данных, функции защиты данных для этого центра данных и его содержимое станут недоступны в расширении.

Если у ID пользователя IBM Spectrum Protect (заданного опцией `VMCUser`) недостаточно полномочий для выполнения операции резервного копирования и восстановления, появится следующее сообщение:

```
ANS9365E Ошибка API VMware vStorage.
"Отказано в разрешении на выполнение этой операции."
```

Если у ID пользователя IBM Spectrum Protect недостаточно полномочий на просмотр компьютера, появятся следующие сообщения:

```
Команда резервного копирования виртуальных машин запущена.  Всего виртуальных машин
для обработки: 1
ANS4155E Не удалось найти виртуальную машину 'tango' на сервере VMware.
ANS4148E Полное резервное копирование виртуальной машины 'foxtrot' завершилось
         неудачно с кодом возврата 4390
```

Более подробную информацию об использовании полномочий смотрите в замечании в разделе **Полномочия сервера vCenter, необходимые для графического интерфейса Data Protection for VMware vSphere и средства перемещения данных**.

Чтобы получить информацию журнала через сервер VMware Virtual Center для устранения проблем с разрешениями, выполните следующие шаги:

1. В окне Параметры сервера vCenter выберите **Опции записи в журнал** и задайте для опции "**Запись в журнал vCenter** значение **Trivia (Trivia)**.
2. Воспроизведите ошибку разрешений.
3. Переустановите для опции **Запись в журнал vCenter** ее предыдущее значение, чтобы запретитмь запись лишней информации журнала.
4. В окне Системные журналы найдите самый последний журнал сервера vCenter (`vpxd-`*`wxyz`*`.log`) и найдите строку `NoPermission`. Например:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Ошибка вызова:
   Сеанс vim.VirtualMachine.createSnapshot: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Сгенерировано: vim.fault.NoPermission
   ```

   Это сообщение журнала указывает, что у ID пользователя нет достаточных полномочий на создание снимка (`createSnapshot`).

Установка компонентов Data Protection for VMware

Вы можете установить все компоненты, которые доступны в пакете Data Protection for VMware для вашей операционной системы, или часть этих компонентов.

Об этой задаче

Используя программу установки Data Protection for VMware можно установить следующие компоненты:

- Агент восстановления IBM Spectrum Protect
- Windows Интерфейс командной строки агента восстановления
- Windows Документация (файл readme и файл замечаний)
- Файл включения Data Protection for VMware
- Графический интерфейс Data Protection for VMware vSphere
- Функцию перемещения данных, которая содержит следующие элементы:
  - Графический интерфейс перемещения данных
  - Веб-клиент перемещения данных
  - Файлы среды выполнения API клиента (64-разрядного)
  - Командная строка клиента администрирования
  - Файлы среды выполнения API VMware vStorage

Если вы хотите установить средство перемещения данных (прокси-сервер монтирования), агент восстановления и необходимые пакеты поддержки, можно выбрать полную установку или использовать опцию Расширенная установка.

Совет: В одной системе можно создать несколько средств перемещения данных в виде программы Data Protection for VMware или можно создать средства перемещения данных в удаленных системах. Такая конфигурация повышает количество ресурсов, доступных для использования компонентом Data Protection for VMware. Системы с установленным средством перемещения данных называются серверами резервного копирования vStorage.

Получение пакета установки Data Protection for VMware

Пакет установки Data Protection for VMware можно получить с сайта скачивания IBM (например, IBM Passport Advantage).

Linux

Прежде чем начать

Если вы собираетесь скачать эти файлы, задайте неограниченный системный предел пользователя для максимального размера файла, чтобы файлы были успешно скачаны:

1. Чтобы запросить значение для максимального размера файла, введите следующую команду:

   ```
   ulimit -Hf
   ```

2. Если системный пользовательский предел на максимальный размер файла не задан неограниченным, измените его на неограниченный, следуя инструкциям в документации для вашей операционной системы.

Процедура

1. Скачайте соответствующий файл пакета с одного из следующих веб-сайтов:
   - При первой установке или при установке нового выпуска перейдите на сайт Passport Advantage по адресу: http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage - единственный сайт, с которого можно загрузить лицензионный файл пакета.
   - Самую свежую информацию, обновления и исправления обслуживания смотрите на сайте поддержки IBM Spectrum Protect: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Если вы скачали пакет с сайта скачивания IBM, то сделайте следующее:
   a. Скачайте файл пакета в каталог по вашему выбору. Путь может содержать не более 40 символов. Убедитесь, что извлекаете файлы установки в пустой каталог. Не выполняйте извлечение в каталог с ранее извлеченными файлами или с какими-либо еще файлами.

   b. Linux Убедитесь, что для пакета заданы разрешения для выполнения. Если нужно, то измените разрешения для файла, введя следующую команду:

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

   c. Linux Извлеките пакет, введя следующую команду:

      ```
      ./имя_пакета.bin
      ```

      где *имя_пакета* - это имя скачанного файла.

   d. Windows Распакуйте пакет, дважды щелкнув по *имя_пакета*, где *имя_пакета* - это имя скачанного файла.

Установка компонентов Data Protection for VMware при помощи мастера установки

Компоненты Data Protection for VMware можно установить при помощи мастера установки.

Об этой задаче

Windows Для установки Data Protection for VMware и средства перемещения данных можно использовать программу установки комплекта (Suite Installer).

Linux Для установки Data Protection for VMware и средства перемещения данных можно использовать автономную программу установки.

Установка Data Protection for VMware в системах Windows

Установите компоненты и функции Data Protection for VMware при помощи мастера установки.

Прежде чем начать

Прежде чем устанавливать компоненты Data Protection for VMware, убедитесь, что вы выполнили следующие требования:

- У ID пользователя есть права доступа администратора.
- Существует сетевое соединение с сервером VMware vCenter Server 6.x или новее с правами доступа администратора.
- Существует сетевое соединение с сервером IBM Spectrum Protect с правом доступа администратора (полномочия **Система** или **Неограниченный домен политики**). Этот сервер должен быть доступен и должен работать.
- Убедитесь, что вы ознакомились со следующими требованиям:
  - “Требования к системе” на стр. 13
  - “Необходимые разрешения на установку” на стр. 18
  - “Необходимые порты связи” на стр. 18

Прежде чем устанавливать Data Protection for VMware, нужно знать о следующих опциях:

Тип установки

Стандартная установка
При стандартной установке устанавливаются все компоненты и функции Data Protection for VMware.

Расширенная установка
В панели Расширенная установка есть опция для установки отдельного средства перемещения данных. Процесс установит в системе средство перемещения данных (прокси-сервер монтирования), агент восстановления и необходимые пакеты поддержки. Используйте эту опцию установки для добавления отдельных узлов перемещения данных. Кроме того, эта опция устанавливает агенты защиты приложений, чтобы разрешить восстановление отдельных баз данных. После установки можно использовать графический интерфейс IBM Spectrum Protect для конфигурирования узла перемещения данных и служб при помощи модуля plug-in VMware vSphere.

Об этой задаче

Для установки Data Protection for VMware можно использовать программу установки комплекта. Файл `spinstall.exe` для программы установки комплекта находится в корне пакета установки.

Список компонентов и функций, которые можно установить, смотрите в разделе “Устанавливаемые компоненты” на стр. 1.

Процедура

Чтобы установить Data Protection for VMware, выполните следующие шаги из расположения файла `spinstall.exe` для компонента, который вы хотите установить:

1. Дважды щелкните по файлу `spinstall.exe`.
2. Следуя инструкциям мастера, установите выбранные компоненты.

Дальнейшие действия

Чтобы получить доступ к Графический интерфейс Data Protection for VMware vSphere, смотрите следующее:

- “Получение доступа к компоненту Графический интерфейс Data Protection for VMware vSphere” на стр. 33

Мастер конфигурации автоматически откроется, когда вы впервые запустите графический интерфейс.

Установка Data Protection for VMware на системах Linux

Установите Data Protection for VMware на системах Linux при помощи режима InstallAnywhere.

Прежде чем начать

Прежде чем устанавливать компонент Data Protection for VMware, убедитесь, что вы выполнили следующие требования:

- Прежде чем продолжить, убедитесь, что у ID пользователя есть необходимый уровень разрешений и что нужные порты связи открыты.
- Процесс установки создает пользователя `tdpvmware`. Все команды **`vmcli`** нужно вводить от имени пользователя `tdpvmware`, а не от имени ID пользователя root.
- При установке в режиме консоли требуется X Window Server.
- Убедитесь, что вы ознакомились со следующими требованиям:
  - “Требования к системе” на стр. 13
  - “Необходимые разрешения на установку” на стр. 18
  - “Необходимые порты связи” на стр. 18

Процедура

Для установки Data Protection for VMware выполните следующие действия:

1. В корне папки установки перейдите в каталог `CD/Linux/DataProtectionForVMware`.
2. В командной строке введите следующую команду:

   ```
   ./install-Linux.bin
   ```

Результаты

Если вы получите какие-либо предупреждения или ошибки, смотрите дополнительную информацию в файлах журналов. Смотрите раздел “Операции файла журнала” на стр. 90.

Если вам не удается установить Data Protection for VMware из-за ошибки, смотрите процедуру "Удалить Data Protection for VMware вручную" в разделе “Деинсталляция Data Protection for VMware в системе Linux” на стр. 40.

Выполнение чистой установки Data Protection for VMware в Linux

Если установка Linux прервалась, то обычно ее можно перезапустить. Однако перезапустить установку не удается, то требуется новая ("чистая") установка.

Об этой задаче

Перед запуском новой установки убедитесь, что, что продукт удален. Чтобы обеспечить чистую среду, сделайте следующее:

Процедура

1. Если компонент Графический интерфейс Data Protection for VMware vSphere установлен, выполните следующие задачи:
   a. Остановите компонент интерфейс командной строки Data Protection for VMware, введя следующую команду:
   `/etc/init.d/vmcli stop`
   b. Остановите веб-сервер графического интерфейса Data Protection for VMware, введя следующую команду:
   `/etc/init.d/webserver stop`
   c. Удалите пакет `.rpm` следующей командой:
   `rpm -e TIVsm-TDPVMwarePlugin`
2. Удалите записи Deployment Engine:
   a. Введите следующую команду, чтобы вывести список всех записей Deployment Engine:
   `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b. Введите следующую команду, чтобы удалить все записи Deployment Engine:
   `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <дискриминант>`
   c. Удалите каталог `/var/ibm/common`.
   d. Удалите каталог `/usr/ibm/common`.
   e. Очистите каталог `/tmp`, удалив файл `acu_de.log` (если он есть).
   f. Удалите каталог `/tmp` , содержащий ID пользователя, установившего Deployment Engine.
   g. Удалите все записи Deployment Engine из системного файла `/etc/inittab`. Эти записи содержатся в блоке `#Begin AC Solution Install block - #End AC Solution Install block`. Удалите весь текст между этими ограничителями и удалите сами ограничители.
   h. Удалите все ссылки Deployment Engine из системного файла `/etc/services`.
3. Удалите все файлы Data Protection for VMware из неудачной установки.
   a. Удалите все файлы из каталога *<USER_INSTALL_DIR>* (каталог, в который выполнялась неудачная установка). Например, `/opt/tivoli/tsm/TDPVMware/`
   b. Удалите все ярлыки рабочего стола.

4. Создайте резервную копию глобального файла реестра (`/var/.com.zerog.registry.xml`). После резервного копирования этого файла удалите все метки, которые ссылаются на Data Protection for VMware.
5. Удалите файлы журнала в корневом каталоге, которые содержат строку `TDPVMware`. Например: `IA-TDPVMware-00.log` или `IA-TDPVMware_Uninstall-00.log`.
6. Удалите пользователя, который запускал компонент интерфейс командной строки Data Protection for VMware.
   a. Введите следующую команду:
      ```
      userdel -r tdpvmware
      ```
   b. Введите следующую команду:
      ```
      groupdel tdpvmware
      ```

      Совет: В некоторых версиях Linux команда **`userdel`** также удаляет и группу, если не существует никакого другого связанного пользователя. Поэтому игнорируйте все сообщения о неудачном завершении, связанные с командой.

Результаты

После выполнения этих действий запустите чистую установку.

Установка компонентов Data Protection for VMware в режиме без вывода сообщений

Можно установить Data Protection for VMware в фоновом режиме. При установке без вывода сообщений сообщения не выводятся.

Об этой задаче

Windows Для установки Data Protection for VMware и средства перемещения данных можно использовать программу установки комплекта (Suite Installer).

Linux Для установки Data Protection for VMware и средства перемещения данных можно использовать автономную программу установки.

Установка Data Protection for VMware в системах Windows в режиме без вывода сообщений

Установите все компоненты Data Protection for VMware и функцию перемещения данных, используя программу установки комплекта в режиме без вывода сообщений.

Прежде чем начать

Прежде чем устанавливать Data Protection for VMware и функцию перемещения данных, убедитесь, что ваша система отвечает требованиям в следующих разделах:

- “Требования к системе” на стр. 13
- “Необходимые разрешения на установку” на стр. 18
- “Необходимые порты связи” на стр. 18

Об этой задаче

Ограничение: Все функции устанавливаются в их расположении по умолчанию. Чтобы найти каталоги установки по умолчанию для компонентов, смотрите подразделы в разделе “Устанавливаемые компоненты” на стр. 1.

Процедура

Для установки Data Protection for VMware выполните следующие действия:

1. Введите в командной строке следующую команду:

   ```
   cd папка_извлечения\TSMVMWARE_WIN
   ```

2. Введите команду

   ```
   spinstall.exe /silent
   ```

   При первом монтировании тома будет показано следующее сообщение:

   ```
   Драйвер виртуальных томов еще не зарегистрирован. Recovery Agent может зарегистрировать
   драйвер сейчас. Во время регистрации может выводиться предупреждение с логотипом
   Microsoft Windows.
   Примите это предупреждение, чтобы можно было выполнить регистрацию.
   Зарегистрировать драйвер виртуальных томов сейчас?
   ```

   Введите **Да**, чтобы зарегистрировать драйвер виртуальных томов.

Задачи, связанные с данной:

“Деинсталляция Data Protection for VMware в Windows в режиме без вывода сообщений” на стр. 39

Установка Data Protection for VMware в системах Linux в режиме без вывода сообщений

Вы можете настроить набор функций Data Protection for VMware, которые следует установить в операционной системе Linux в режиме без вывода сообщений.

Прежде чем начать

Прежде чем устанавливать компонент Data Protection for VMware, убедитесь, что вы выполнили следующие требования:

- Прежде чем продолжить, убедитесь, что у ID пользователя есть необходимый уровень разрешений и что нужные порты связи открыты.
- Процесс установки создает пользователя `tdpvmware`. Все команды **`vmcli`** нужно вводить от имени пользователя `tdpvmware`, а не от имени ID пользователя root.
- При установке в режиме консоли требуется X Window Server.
- Убедитесь, что вы ознакомились со следующими требованиям:
  - “Требования к системе” на стр. 13
  - “Необходимые разрешения на установку” на стр. 18
  - “Необходимые порты связи” на стр. 18

Об этой задаче

В Data Protection for VMware есть следующие функции установки в режиме без вывода сообщений для операционных систем Linux:

Таблица 7. Компоненты Data Protection for VMware для установки без вывода сообщений

Функция	Описание	Устанавливается по умолчанию?
Docs	Файл Readme	Да

Таблица 7. Компоненты Data Protection for VMware для установки без вывода сообщений (продолжение)

Функция	Описание	Устанавливается по умолчанию?
TDPVMwareDM	Установка этой функции включает в себя файл поддержки возможностей. Разрешает IBM Spectrum Protect выполнять следующие типы резервного копирования: • Периодическое инкрементное резервное копирование виртуальной машины • Полное резервное копирование виртуальной машины Всегда инкрементное • Инкрементное резервное копирование виртуальной машины Всегда инкрементное Если вы выгружаете рабочие нагрузки резервного копирования, то этот файл нужно установить на сервере резервного копирования vStorage.	Да
TDPVMwareGUI	Графический интерфейс Data Protection for VMware vSphere. **Примечание:** Также включает в себя установку файла поддержки возможностей.	Нет

Процедура

Чтобы установить Data Protection for VMware, выполните следующие шаги из каталога, куда вы распаковали пакет установки:

1. Откройте файл *путь*`../Linux/DataProtectionForVMware/installer.properties` и раскомментируйте следующую запись, чтобы принять лицензию (где *путь* - это папка установки):

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. Выберите один из следующих методов установки компонентов Data Protection for VMware:
   - Для установки по умолчанию откройте папку `CD/Linux/DataProtectionForVMware` и введите следующую команду:

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - Для пользовательской установки выполните следующие шаги:
     a. Задайте в файле `installer.properties` подходящие значения:
        1) Обозначение **`INSTALL_MODE=Custom`**. Убедитесь, что знак номера (#) удален из этого оператора.
        2) Укажите, какие функции следует установить, используя опцию **`CHOSEN_INSTALL_FEATURE_LIST`**. Например, чтобы установить все компоненты, задайте следующее:

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. В папке `CD/Linux/DataProtectionForVMware` введите следующую команду:

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

Первые шаги после установки Data Protection for VMware

После установки компонента Data Protection for VMware подготовьтесь к конфигурированию. Использование мастера по конфигурированию - предпочтительный способ конфигурирования компонента Data Protection for VMware.

Рабочая таблица конфигурации

Используйте этот контрольный список для записи информации, которая вам потребуется при конфигурировании и администрировании Data Protection for VMware. Контрольный список поможет вам вспомнить указанные значения после конфигурирования.

Таблица 8. Рабочая таблица конфигурации Data Protection for VMware

Элемент	Собственное значение	Примечания
Информация о сервере IBM Spectrum Protect		
Адрес сервера IBM Spectrum Protect		
Порт сервера IBM Spectrum Protect		
ID администратора сервера/пароль IBM Spectrum Protect		
Порт администратора сервера IBM Spectrum Protect		
Опции определений узлов		
Префикс для добавления на узлы		
Домен политики, который нужно использовать при регистрации новых узлов		
Имя узла/пароль vCenter		
Имя узла/пароль VMCLI		
Имена узлов/пароли центра данных **Напоминание:** Можно создать несколько узлов центра данных.		Имя узла центра данных состоит из заданного префикса, после которого стоит символ подчеркивания, а затем - имя центра данных. Например: *nodePrefix_datacenterName*
Имена/пароли узлов перемещения данных на сервере резервного копирования vStorage **Напоминание:** Можно создать несколько узлов перемещения данных.		Узел средства перемещения данных состоит из имени узла центра данных, после которого стоит символ подчеркивания, а затем - `DM`. Например: *datacenterNodename*_DM
Имена/пароли узлов перемещения данных на удаленных серверах **Напоминание:** Можно создать несколько узлов перемещения данных, не находящихся на сервере резервного копирования vStorage.		
Прокси-узел монтирования Прокси-узел монтирования используется при восстановлении данных.	Windows: Linux:	

Получение доступа к компоненту Графический интерфейс Data Protection for VMware vSphere

Используйте компонент Графический интерфейс Data Protection for VMware vSphere для резервного копирования, восстановления и управления виртуальными машинами в среде VMware vCenter.

Прежде чем начать

Прежде чем вы сможете получить доступ к компоненту Графический интерфейс Data Protection for VMware vSphere во время установки, нужно выбрать опцию для защиты ваших данных в среде vSphere.

Процедура

- Если при установке вы выберете опцию **Разрешить доступ к графическому интерфейсу через веб-браузер**, вы сможете получить доступ к компоненту Графический интерфейс Data Protection for VMware vSphere из браузера:
  1. Откройте браузер и введите следующий URL:

     `https://`*`имя_хоста`*`:`*`порт`*`/TsmVMwareUI`

     Здесь используются следующие обозначения:
     - *имя_хоста* - имя системы, где установлен Графический интерфейс Data Protection for VMware vSphere.
     - *порт* - номер порта, через который доступен графический интерфейс vSphere. Номер порта по умолчанию - 9080. Номер защищенного порта по умолчанию - 9081.
  2. Войдите при помощи своего ID пользователя и пароля vCenter.
- Если при установке вы не выберете опцию **Разрешить доступ к графическому интерфейсу через веб-браузер**, вы можете запустить Графический интерфейс Data Protection for VMware vSphere, выполнив следующие шаги:
  1. Откройте клиент VMware vSphere и войдите в систему, используя ID пользователя и пароль vCenter.
  2. В панели Решения и приложения клиента vSphere щелкните по значку Графический интерфейс Data Protection for VMware vSphere.

Обновление Data Protection for VMware

Можно обновить Data Protection for VMware от предыдущей версии программы.

Информацию о совместимости с более ранними версиями смотрите в техническом замечании 1993819.

Обновление версии 7.1.8: Если в процессе обновления появится сообщение, в котором вас спросят, хотите ли вы переопределить существующий файл `jextract`, выберите **Да дла всех**.

Обновление Data Protection for VMware

В этой процедуре рассказывается, как произвести обновление до Data Protection for VMware V8.1.7.

Прежде чем начать

Важное замечание: Эта процедура обновления применяется к системе, в которой не установлен IBM Spectrum Protect Snapshot for VMware.

Для обновления Data Protection for VMware требуются полномочия администратора.

Обновления существующего компонента Графический интерфейс Data Protection for VMware vSphere обрабатываются следующим образом:

- Прежде чем начнется процесс обновления компонента Графический интерфейс Data Protection for VMware vSphere, создается резервная копия файлов параметров.
- Используются те же номера порта базы данных Derby и базового порта по умолчанию WebSphere Application Server.
- Linux Значения в профиле (`vmcliprofile`) используются для интерфейс командной строки Data Protection for VMware.

Ограничение:

- Windows При установке компонента IBM Spectrum Protect for Virtual Environments в расположение, не являющееся расположением по умолчанию, процесс обновления устанавливает функции IBM Spectrum Protect for Virtual Environments V8.1.7 в каталог установки по умолчанию. Произвести обновление в расположение, не являющееся расположением по умолчанию, нельзя. Информацию о каталогах установки по умолчанию для каждой функции смотрите в подразделах раздела “Устанавливаемые компоненты” на стр. 1.
- Linux Windows Процесс обновления не устанавливает новые компоненты. Например, если в предыдущей версии был установлен только графический интерфейс агент восстановления, процедура обновления не установит интерфейс командной строки компонента агент восстановления. В этом случае запустите программу установки и выберите для установки отсутствующий компонент.
- Linux Компонент агент восстановления в версии Linux должен относиться к той же версии, что и компонент агент восстановления в прокси-системе Windows. Поэтому, если вы обновите компонент агент восстановления в Linux, вы также должны обновить версию агент восстановления в прокси-системе Windows.

Процедура

Для обновления Data Protection for VMware сделайте следующее:

1. Остановите все работающие у вас компоненты и службы Data Protection for VMware.
2. Размонтируйте все смонтированные виртуальные тома. Размонтировать тома можно с помощью графического интерфейса агент восстановления или интерфейса командной строки (команда **`mount del`**).
3. Следуйте инструкциям в “Установка Data Protection for VMware в системах Windows” на стр. 26.

Примечание: Linux Если у вас установлено средство перемещения данных V6.x, вы должны его деинсталлировать, прежде чем устанавливать V8.1.7. Следуйте инструкциям в разделе Деинсталляция клиента IBM Spectrum Protect Linux x86_64.

4. Скачайте пакет кодов.
5. Запустите процесс обновления из папки, где вы сохранили этот пакет кода.

   a. Windows Запустите файл `spinstall.exe`.

   b. Linux Запустите файл `install-Linux.bin`.

   На компьютере можно установить только один компонент Графический интерфейс Data Protection for VMware vSphere. Поэтому на одном и том же компьютере не допускается более одного компонента Графический интерфейс Data Protection for VMware vSphere.

Обновление Data Protection for VMware в 64-разрядной системе Windows в режиме без вывода сообщений

Можно обновить Data Protection for VMware в режиме без вывода сообщений в поддерживаемой 64-разрядной операционной системе

Прежде чем начать

При установке компонента Data Protection for VMware V6.x в расположение, не являющееся расположением по умолчанию, процесс обновления в режиме без вывода сообщений устанавливает функции Data Protection for VMware V8.1.7 в каталог установки по умолчанию. Произвести обновление в режиме без вывода сообщений в расположение, не являющееся расположением по умолчанию, нельзя. Информацию о каталогах установки по умолчанию для каждой функции смотрите в подразделах раздела “Устанавливаемые компоненты” на стр. 1.

Процедура

Для обновления Data Protection for VMware сделайте следующее:

1. Остановите все работающие компоненты Data Protection for VMware.
2. Размонтируйте все смонтированные виртуальные тома. Размонтировать тома можно с помощью графического интерфейса агент восстановления или интерфейса командной строки (команда **mount del**).
3. Размонтируйте все смонтированные виртуальные тома. Размонтировать тома можно с помощью графического интерфейса агент восстановления или интерфейса командной строки (команда **mount del**).
4. Скачайте пакет кодов.
5. Перейдите в папку Data Protection for VMware.
6. В окне командной строки введите следующую команду: `spinstall.exe /silent GUI_MODE=vcenter DIRECT_START=1 VCENTER_HOSTNAME=<имя_хоста> VCENTER_USERNAME=<имя_пользователя> VCENTER_PASSWORD=<пароль> /debuglog <путь_к_файлу>`

Обновление Data Protection for VMware в Linux в режиме без вывода сообщений

Можно обновить Data Protection for VMware в поддерживаемой операционной системе Linux в режиме без вывода сообщений.

Об этой задаче

Используйте в сочетании с функцией установки без вывода сообщений следующие параметры компонента Data Protection for VMware:

Таблица 9. Параметры Data Protection for VMware для обновления установки без вывода сообщений

Параметр	Описание	Значение по умолчанию
VCENTER_HOSTNAME	Полное имя домена или IP-адрес сервера vCenter.	Нет
VCENTER_USERNAME	ID пользователя vCenter. Этот ID пользователя должен быть администратором VMware, у которого есть разрешение на регистрацию и дерегистрацию расширений.	Нет
VCENTER_PASSWORD	Пароль vCenter.	Нет
DIRECT_START	Чтобы получить доступ к Графический интерфейс Data Protection for VMware vSphere в веб-браузере, укажите **DIRECT_START=YES**. Доступ к компоненту Графический интерфейс Data Protection for VMware vSphere производится через закладку URL на веб-сервере графического интерфейса. Если вы не хотите получать доступ к Графический интерфейс Data Protection for VMware vSphere в веб-браузере, укажите **DIRECT_START=NO**.	YES **Важное замечание:** По завершении обновления изменить значение **DIRECT_START** будет нельзя; чтобы это сделать, придется переустановить продукт.

Процедура

Для обновления Data Protection for VMware выполните следующие действия:

1. Убедитесь, что нет активных сеансов резервного копирования, восстановления или монтирования.
2. Убедитесь что все существующие графические интерфейсы Графический интерфейс Data Protection for VMware vSphere или агент восстановления закрыты.
3. Скачайте пакет кода.
4. В папке Data Protection for VMware перейдите в папку Linux.
5. Введите в окне командной строки команду `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` с предпочтительными параметрами.
   Например: `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username -VCENTER_PASSWORD=password -DIRECT_START=yes -REGISTER_PLUGIN=yes`

Обновление Data Protection for VMware в среде связанного режима сервера vCenter

Все хосты графического интерфейса пользователя Data Protection for VMware должны быть своевременно обновлены, чтобы включить компоненты Data Protection for VMware для поддержки текущих возможностей связанного режима VMware

Об этой задаче

Примечание: Эта информация относится к версиям 6.0, 6.5 и 6.7 прикладной программы vSphere, работающей на VMware vCenter.

Связанный режим сервера VMware vCenter - это инструмент, который предоставляет обзор зон управления, так что серверы могут поддерживать больше виртуальных машин. Подключаемый модуль IBM Spectrum Protect Data Protection for VMware совместим с VMware, работающим в связанном режиме. Дополнительную информацию об этой возможности VMware смотрите в документации VMware в разделе Улучшенный связанный режим vCenter.

Когда vCenter работают в связанном режиме, в пользовательском интерфейсе vSphere доступно единое представление всех vCenter. Тот же пользовательский интерфейс доступен с любого из связанных друг с другом vCenter. В результате подключаемый модуль IBM Spectrum Protect Data Protection выводится на всех vCenter, даже если он установлен и сконфигурирован на одном vCenter.

Этот подключаемый модуль виден на каждом vCenter, но его функциональные возможности доступны только на тех vCenter, у которых есть связанный с ними хост графического пользовательского интерфейса IBM Spectrum Protect Data Protection for VMware.

При обновлении среды связанного режима сервера vCenter имейте в виду следующие вопросы:

- При использовании vCenter в связанном режиме первое обновление одного из vCenter приведет к тому, что подключаемый модуль нового уровня станет видимым со всех связанных vCenter. Подключаемый модуль IBM Spectrum Protect Data Protection for VMware разработан как совместимый с хостом графического пользовательского интерфейса более раннего уровня. Например, подключаемый модуль Data Protection for VMware V8.1.6 остается совместимым с хостом графического пользовательского интерфейса Data Protection for VMware V8.1.4.
- Хост графического пользовательского интерфейса более раннего уровня все еще будет работать с новым подключаемым модулем, но функции, введенные в новом выпуске, работать не будут. Надо своевременно выполнить обновление всех хостов графического пользовательского интерфейса, чтобы использовать все функциональные возможности нового подключаемого модуля.

Пример

До обновления до Версии 8.1.6 vCenter1 и vCenter2 работали в связанном режиме. У каждого из них есть хоста графического пользовательского интерфейса IBM Data Protection for VMware. Этот подключаемый модуль в vSphere и хосты графического пользовательского интерфейса работают в Версии 8.1.4.

vCenter1 обновляется до V8.1.6. Теперь этот подключаемый модуль и хоста графического пользовательского интерфейса host1 находятся на уровне V8.1.6. Пользователь, который входит в систему vSphere для vCenter2, будет видеть подключаемый модуль V8.1.6, а не подключаемый модуль V8.1.4. Этот пользователь

| может выбрать в **IBM Spectrum Protect -> Конфигурировать -> Соединения** и увидеть, что vCenter1 использует хост графического пользовательского интерфейса V8.1.6, но хост графического пользовательского интерфейса vCenter2 по-прежнему использует V8.1.4.

| Подключаемый модуль Spectrum Protect по-прежнему работает для vCenter2 точно так же, как он работал для V8.1.4. Разница в том, что никакие новые возможности V8.1.6 нельзя использовать в vCenter2 - они работают только в vCenter1, пока не будет выполнено обновление хоста графического пользовательского интерфейса до V8.1.6.

Деинсталляция Data Protection for VMware

Процесс деинсталляции Data Protection for VMware аналогичен процессам новой установки и обновления версии.

Деинсталляция Data Protection for VMware в Windows

Деинсталлируйте компоненты Data Protection for VMware и удалите файлы и каталоги из системы Windows.

Прежде чем начать

Чтобы обеспечить успешную деинсталляцию, выполните следующие рекомендации:

- Если компонент IBM Spectrum Protect vSphere Client - Модуль plugin используют другие хосты графического веб-интерфейса компонента Data Protection for VMware, не дерегистрируйте расширение веб-клиента.

Об этой задаче

После завершения деинсталляции файлы конфигурации и файлы свойств находятся в каталоге `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config`.

Процедура

1. Остановите все работающие компоненты Data Protection for VMware.
2. Размонтируйте все смонтированные виртуальные тома.
3. Удалите все существующие резервные копии виртуальной машины, используя команду `delete backup` средства перемещения данных.
4. Удалите все установленные службы перемещения данных с помощью команды `dsmcutil remove`.

   Чтобы получить список служб, перейдите в каталог `C:\Program Files\Tivoli\TSM\baclient\` и введите команду: `dsmcutil list`.

   Удалите службы с помощью команд, аналогичных следующим, подставив имя перечисленной службы в кавычках:

   ```
   dsmcutil remove /name:"TSM Remote Client Agent"
   dsmcutil remove /name:"TSM Client Acceptor"
   ```

5. Выберите **Пуск > Панель управления > Программы и компоненты > Деинсталлировать программу**. Деинсталлируйте следующие программы:
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - Лицензия IBM Spectrum Protect for Virtual Environments Data Protection for VMware
   - IBM Spectrum Protect JVM

6. Удалите из файловой системы следующие файлы и каталоги Data Protection for VMware (если они есть). В случае IBM Spectrum Protect for Virtual Environments V8.1.6 и новее удалите:

   ```
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   ```

   Можно также удалить:

   ```
   C:\Program Files\Tivoli\TSM
   ```

   если оставшиеся файлы журналов и файлы конфигурации больше не нужны. Если вы хотите сохранить эти файлы, они будут находиться в каталоге `C:\Program Files\Tivoli\TSM\baclient`. В случае IBM Spectrum Protect for Virtual Environments V8.1.4 и более ранних версий удалите:

   ```
   C:\IBM\tivoli
   C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
   C:\Program Files\Common Files\Tivoli
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   ```

   Можно также удалить:

   ```
   C:\Program Files\Tivoli\TSM
   ```

   если оставшиеся файлы журналов и файлы конфигурации больше не нужны. Если вы хотите сохранить эти файлы, они будут находиться в каталоге `C:\Program Files\Tivoli\TSM\baclient`.

Дальнейшие действия

Убедитесь, что все компоненты удалены из системы.

Деинсталляция Data Protection for VMware в Windows в режиме без вывода сообщений

Вы можете деинсталлировать Data Protection for VMware в режиме без вывода сообщений в операционной системе Windows.

Об этой задаче

После завершения деинсталляции файлы конфигурации и файлы свойств находятся в каталоге `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config`.

Процедура

Чтобы деинсталлировать Data Protection for VMware, сделайте следующее:

1. Остановите все работающие компоненты Data Protection for VMware.
2. Размонтируйте все смонтированные виртуальные тома. Размонтировать тома можно с помощью графического интерфейса агент восстановления или интерфейса командной строки (команда **mount del**).
3. В окне командной строки используйте команду **cd**, чтобы перейти в одну из следующих папок:
   - Чтобы настроить операцию деинсталляции, перейдите в папку `X64`.

- Чтобы деинсталлировать Data Protection for VMware с помощью программы установки комплекта (Suite Installer), выберите <точная папка>TSM4VE_WIN.

4. В окне командной строки выполните следующую команду:
   - Для пользовательской операции деинсталляции выберите одну из следующих команд:
     – Введите эту команду, чтобы деинсталлировать Data Protection for VMware и дерегистрировать Графический интерфейс Data Protection for VMware vSphere:

       ```
       spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
       VCENTER_HOSTNAME=<имя хоста или IP-адрес vCenter>
       VCENTER_USERNAME=<имя пользователя vCenter>
       VCENTER_PASSWORD=<пароль vCenter>"
       ```

   - Чтобы деинсталлировать все функции с помощью программы установки комплекта, введите следующую команду:

     ```
     spinstall.exe /silent /remove
     ```

5. По завершении деинсталляции перезапустите систему.

Деинсталляция Data Protection for VMware в системе Linux

Деинсталлируйте Data Protection for VMware и удалите файлы и каталоги из поддерживаемой операционной системы Linux.

Прежде чем начать

Чтобы обеспечить успешную деинсталляцию, выполните следующие рекомендации:

- Удалите узлы с сервера IBM Spectrum Protect. Это нужно сделать до деинсталляции продукта Data Protection for VMware:
  1. Запустите dsmadmc из /opt/tivoli/tsm/client/ba/bin/dsmadmc.
  2. Возможно, вам потребуется использовать команду del, чтобы удалить файловое пространство для узлов: del file *имя_узла* *
  3. Используйте команду q для запроса информации для узлов: q filespace *имя_узла* *
  4. Используйте команду rem, чтобы удалять узлы: rem node *имя_узла*
- Остановите службы dsmcad, созданные для функций перемещения данных. Используйте инструкции, содержащиеся в техническом замечании http://www-01.ibm.com/support/docview.wss?uid=swg21358414
  1. При помощи команды ps проверьте, работает ли служба dsmcad: ps -ef|grep dsmcad
  2. При помощи команды kill остановите службу dsmcad: kill -9 *ID_процесса_dsmcad*
- Нужно стереть файлы, связанные с созданием служб перемещения данных. Перейдите в каталог установки и введите следующую команду:

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  Нажмите клавишу Enter, чтобы выбрать имя узла, и снова нажмите клавишу Enter, чтобы его удалить.

  Имена узлов можно найти в файле dsm.sys.
- При деинсталляции компонента IBM Spectrum Protect vSphere Client - Модуль plugin из среды VMware vSphere 5.5 удаляются только связанные с ним метки полномочий и описания. Фактические полномочия останутся установленными. Эта проблема - известное ограничение VMware. Для получения дополнительной информации смотрите следующую статью в базе знаний VMware: http://kb.vmware.com/kb/2004601.

- Файл разблокирования Data Protection for VMware не удаляется после деинсталляции продукта.

Об этой задаче

Если вы деинсталлируете Data Protection for VMware в Linux, то по умолчанию тип деинсталляции - это тот же процесс, что и тип установки. Чтобы использовать другой процесс деинсталляции, задайте правильный параметр. Например, если вы использовали установку без вывода сообщений, то вы можете использовать для деинсталляции мастер установки, указав параметр `-i swing`. Запустите процесс деинсталляции от имени пользователя root. Надо применить профиль пользователя root. Если вы получаете права пользователя root при помощи команды `su`, используйте эту команду `su -` для применения профиля root.

Если процесс деинсталляции начинает удаление файлов программы, то отмена процесса деинсталляции не возвращает систему в 'чистое' состояние. Это может привести к тому, что попытка переустановки завершится неудачно. Поэтому очистите систему, выполнив задачи, описанные в разделе “Удаление компонента Data Protection for VMware вручную из системы Linux” на стр. 42.

Чтобы деинсталлировать Data Protection for VMware, выполните следующие шаги:

Процедура

1. Перейдите в каталог программы деинсталляции. Каталог программы деинсталляции по умолчанию: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. В зависимости от типа установки, используйте один из следующих методов деинсталляции Data Protection for VMware:

   Примечание: Указанные здесь команды нужно вводить в одной строке. В примерах показано две строки для соответствия формату страницы.

   - Чтобы использовать для деинсталляции Data Protection for VMware мастер установки, введите следующую команду:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```

   - Чтобы использовать для деинсталляции Data Protection for VMware консоль, введите следующую команду:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```

   - Чтобы деинсталлировать Data Protection for VMware без вывода сообщений, введите следующую команду:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     Файл `uninstall.properties` содержит информацию о соединении с vCenter. Эта информация необходима для деинсталляции Графический интерфейс Data Protection for VMware vSphere.

Удаление компонента Data Protection for VMware вручную из системы Linux

Об этой задаче

Если Data Protection for VMware нельзя деинсталлировать, используя стандартную процедуру деинсталляции, вы должны вручную удалить Data Protection for VMware из системы, как описано в следующих шагах. Эту процедуру нужно выполнять от имени пользователя root.

Процедура

1. Если вы установили Графический интерфейс Data Protection for VMware vSphere, удалите его пакет из базы данных менеджера пакетов (Package Manager) с помощью команды:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Удалите API IBM Spectrum Protect следующей командой:

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Удалите записи продукта из Deployment Engine:

   a. Введите следующую команду, чтобы просмотреть список всех записей:

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b. Введите следующую команду, чтобы удалить записи установленных модулей, которые связаны с Data Protection for VMware:

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <дискриминант>
      ```

      Убедитесь, что удалены следующие записи блоков:

      ```
      FBJRE
      TDPVMwareGUI
      JavaHelp
      TDPVMwareDM
      ```

      По завершении работы программы деинсталляции удалите следующие каталоги (если они есть):

      - `/opt/tivoli/tsm/client`
      - `/opt/tivoli/tsm/tdpvmware`

      Удалите пользователя `tdpvmware` и связанные с ним каталоги:

      - `userdel tdpvmware`
      - `/home/tdpvmware`
      - `/etc/adsm`

4. Создайте резервную копию глобального файла реестра (`/var/.com.zerog.registry.xml`). После резервного копирования файла удалите все теги, связанные с Data Protection for VMware.
5. Удалите все файлы в каталоге установки (`/opt/tivoli/tsm/tdpvmware`). Также удалите все ярлыки, которые есть на рабочем столе.
6. Создайте резервную копию файлов журналов, находящихся в каталоге `/root` и содержащих `TDPVMware` в имени файла. Например, `IA-TDPVMware-00.log` или `IA-TDPVMware_Uninstall-00.log`. После создания копий удалите эти файлы журнала. Удаляя их, вы сможете увидеть все ошибки, которые будут сгенерированы, если процесс установки снова завершится неудачно.
7. Теперь можно снова установить продукт, как описано в разделе “Установка Data Protection for VMware на системах Linux” на стр. 27.

Изменение существующей установки компонента Data Protection for VMware

В этом разделе представлены инструкции по изменению пакетов и компонентов в существующей установке Data Protection for VMware.

Используя программу установки комплекта (Suite Installer), можно изменить то, какие основные пакеты установлены в системе. Чтобы изменить любой из отдельных компонентов пакета, можно использовать окно **Программы и компоненты** в панели управления Windows.

Изменение пакетов в существующей установке компонента Data Protection for VMware

Чтобы внести изменения в пакеты в существующей установке компонента Data Protection for VMware, можно использовать программу установки комплекта (Suite Installer).

Прежде чем начать

Прежде чем воспользоваться программой установки комплекта, убедитесь, что у вас под рукой есть исходный носитель. Исполняемый файл `spinstall.exe` для программы установки комплекта находится в корне пакета установки.

Об этой задаче

Используйте программу установки комплекта (Suite Installer), чтобы изменить то, какие пакеты устанавливаются в существующей установке компонента Data Protection for VMware. Вы можете добавить или удалить:

- Узел перемещения данных
- Data Protection for VMware

Сделайте следующее:

Процедура

1. Дважды щелкните по файлу `spinstall.exe`, чтобы запустить пакет программы установки комплекта (Suite Installer).
2. Используйте переключатели пакетов в панели **Пользовательская установка**, чтобы определить, какие пакеты нужно установить.
3. Выберите пакеты, необходимые для данной установки.

Изменение компонентов в существующей установке компонента Data Protection for VMware

Чтобы внести изменения в компоненты в существующей установке компонента Data Protection for VMware, можно использовать панель управления Программы и компоненты в Windows.

Прежде чем начать

Прежде чем изменять пакет установки, убедитесь, что у вас под рукой есть исходный носитель.

Об этой задаче

Используйте Windows, чтобы изменить то, какие отдельные компоненты пакета доступны в существующей установке Data Protection for VMware. Можно изменить компоненты:

- На узле перемещения данных
- Data Protection for VMware

Сделайте следующее:

Процедура

1. В разделе **Программы и компоненты панели управления** Windows щелкните правой кнопкой мыши по приложению IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
2. Щелкните по **Изменить**, чтобы обновить установленые в данный момент компоненты пакета.
3. Выберите компоненты, необходимые для данной установки.

Глава 2. Конфигурирование Data Protection for VMware

В этом разделе содержатся инструкции по конфигурированию Data Protection for VMware и по запуску связанных служб.

Совет: После установки Data Protection for VMware инструмент IBM License Metric Tool учитывает узел перемещения данных, только если он подключен к серверу IBM Spectrum Protect и используется для операций с данными. Соответственно, этот узел перемещения данных всегда включается в вычисления лицензий. Узлы перемещения данных, не подключенные к серверу и не используемые для операций с данными, исключаются из вычислений лицензий.

Конфигурирование новой установки при помощи мастера

Используйте мастер конфигурирования для первоначального конфигурирования или внесения незначительных изменений.

Прежде чем начать

У системы, в которой установлен компонент Data Protection for VMware, должно быть сетевое соединение со следующими серверами:

- Сервер резервного копирования vStorage
- Сервер IBM Spectrum Protect
- Сервер vCenter

Об этой задаче

Чтобы сконфигурировать среду компонента Data Protection for VMware, выполните следующие шаги:

Процедура

1. Откройте браузер и введите адрес веб-сервера графического интерфейса: Например:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

2. Войдите в систему с именем пользователя и паролем vCenter.
3. В окне Начинаем работу перейдите в окно Конфигурация и щелкните по **Запустить мастер конфигурирования**.
4. Выполните инструкции на каждой странице мастера; по окончании откроется окно Сводка. Проверьте параметры и нажмите **Готово**, чтобы завершить конфигурирование и закрыть мастер.

   Совет: Информация о каждой странице конфигурации представлена в электронной справке, устанавливаемой вместе с графическим интерфейсом. Щелкните по **Узнать подробнее** в любом из окон графического интерфейса, чтобы открыть электронную справку и получить помощь по задачам. Смотрите раздел *Запуск мастера конфигурирования*.
5. Убедитесь, что узлы перемещения данных правильно сконфигурированы:
   a. Щелкните по вкладке **Конфигурация**, чтобы увидеть страницу Состояние конфигурации.

b. На странице Состояние конфигурации выберите узел перемещения данных, чтобы просмотреть информацию о состоянии в панели Сведения о состоянии. Если для узла показаны предупреждение или ошибка, щелкните по этому узлу и используйте информацию в панели Сведения о состоянии, чтобы устранить ошибку. После этого выберите узел и щелкните по **Проверить выбранный узел**, чтобы проверить, исправлена ли ошибка. Щелкните по **Обновить**, чтобы заново протестировать все узлы.

Результаты

Быстрый путь: После успешного выполнения этой задачи никакое дополнительное конфигурирование для резервного копирования данных виртуальной машины не требуется.

Использование блокнота для изменения существующей установки

Используйте блокнот Изменить конфигурацию, чтобы изменить существующие параметры конфигурации.

Прежде чем начать

Блокнот Изменить конфигурацию дает возможность выполнить следующие операции с конфигурацией:

- Задать или изменить ID администратора IBM Spectrum Protect.
- Переустановить пароль и разблокировать узел VMCLI.
- (Среда vSphere) Добавьте центры данных VMware в ваш домен компонента Графический интерфейс Data Protection for VMware vSphere или удалите их оттуда.
- Добавить или удалить прокси-узлы монтирования. Измените пароль для существующего узла прокси монтирования.
- Добавить или удалить узлы перемещения данных. Измените пароль для существующего узла перемещения данных.
- Разрешить восстановление файлов.
- Включить поддержку тегов для узла перемещения данных.

Об этой задаче

Чтобы изменить существующую конфигурацию, выполните следующие шаги:

Процедура

1. Откройте браузер и введите адрес веб-сервера графического интерфейса: Например:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   Войдите в систему с именем пользователя и паролем vCenter.
2. В окне Начинаем работу перейдите в окно Конфигурация и щелкните по **Правка конфигурации**.
3. Перейдите на подходящую страницу и следуйте инструкциям. Прежде чем переходить на другую страницу Параметры конфигурации, нужно нажать на **OK**, чтобы сохранить свои изменения. В противном случае ваши изменения не вступят в силу.

   Важное замечание: Информация о каждой странице конфигурации представлена в электронной справке, устанавливаемой вместе с графическим интерфейсом.

Щелкните по **Узнать подробнее** в любом из окон графического интерфейса, чтобы открыть электронную справку и получить помощь по задачам. Смотрите раздел *Изменение существующей конфигурации*.

Результаты

Обновленные параметры появятся в окне Конфигурация.

Как включить среду для операций восстановления файлов

Windows

Если администратор разрешил функцию восстановления файлов, то владельцы файлов могут восстанавливать файлы без посторонней помощи.

Прежде чем начать

Если вы не проверили, выполнены ли все обязательные требования, смотрите раздел требований к восстановлению файлов в публикации *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Руководство пользователя*.

Об этой задаче

Выполните следующие шаги в системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere.

Процедура

1. Запустите Графический интерфейс Data Protection for VMware vSphere, открыв веб-браузер и введя адрес веб-сервера графического интерфейса. Например:

   ```
   https://<адрес веб-сервера
   графического интерфейса>:
   9081/TsmVMwareUI/
   ```

   Войдите в систему с ID пользователя и паролем vCenter.
2. В окне Начинаем работу щелкните по **Конфигурация** и выберите одну из следующих задач в списке Задачи:
   - Если вы конфигурируете новую среду, выполните следующие шаги:
     a. Выберите **Запустить мастер конфигурирования клиента**.
     b. Выполните инструкции на каждой странице мастера. Заполните страницу Восстановление файлов, соблюдая следующие рекомендации:
        1) Выберите опцию **Разрешить восстановление файлов**.
        2) Введите контактную информацию администратора, которая показана в интерфейсе восстановления файлов. Если вы не хотите предоставлять контактную информацию, то снимите пометку с переключателя.
        3) Если среда содержит резервные копии виртуальных машин Windows, то введите идентификационные данные пользователя домена Windows. В иных случаях снимите пометку с переключателя и не вводите идентификационные данные.

           Совет: Операция восстановления файлов использует идентификационные данные пользователя домена для получения доступа к совместно используемым сетевым ресурсам на удаленной виртуальной машине. Если среда содержит резервные копии виртуальных машин Windows и никаких идентификационных данных не

введено или введены неправильные идентификационные данные, операция завершится неудачно. Поэтому снимайте пометку с переключателя, только если резервных копий виртуальных машин Windows нет.

4) Щелкните по URL интерфейса восстановления файлов, чтобы проверить, доступен ли интерфейс.

Напоминание: Запишите URL интерфейса восстановления файлов. Владелец гостевой виртуальной машины обращается к интерфейсу восстановления файлов через этот URL.

5) Щелкните по **ОК**, чтобы сохранить изменения.

- Если вы обновляете существующую среду, выполните следующие шаги:
  a. Щелкните по **Изменить конфигурацию TSM**.
  b. На странице Восстановление файлов используйте следующие рекомендации:
     1) Выберите опцию **Разрешить восстановление файлов**.
     2) Введите контактную информацию администратора, которая показана в интерфейсе восстановления файлов. Если вы не хотите предоставлять контактную информацию, то снимите пометку с переключателя.
     3) Если среда содержит резервные копии виртуальных машин Windows, то введите идентификационные данные пользователя домена Windows. В иных случаях снимите пометку с переключателя и не вводите идентификационные данные.

        Совет: Операция восстановления файлов использует идентификационные данные пользователя домена для получения доступа к совместно используемым сетевым ресурсам на удаленной виртуальной машине. Если среда содержит резервные копии виртуальных машин Windows и никаких идентификационных данных не введено или введены неправильные идентификационные данные, операция завершится неудачно. Поэтому снимайте пометку с переключателя, только если резервных копий виртуальных машин Windows нет.

     4) Щелкните по URL интерфейса восстановления файлов, чтобы проверить, доступен ли интерфейс.

        Напоминание: Запишите URL интерфейса восстановления файлов. Владелец гостевой виртуальной машины обращается к интерфейсу восстановления файлов через этот URL.

     5) Щелкните по **ОК**, чтобы сохранить изменения.

Результаты

В среде разрешены операции восстановления файлов. Владельцы файлов могут восстанавливать свои файлы, используя URL для доступа к интерфейсу восстановления файлов IBM Spectrum Protect.

Настройка операций восстановления файлов в Linux

Linux

Чтобы включить функцию восстановления файлов, если компонент Data Protection for VMware установлен в системе Linux, нужно настроить в системе Windows дополнительную среду Data Protection for VMware.

Об этой задаче

При работе с компонентом Data Protection for VMware в среде Linux функция восстановления файлов должна быть установлена в системе Windows, чтобы включить функцию восстановления файлов.

Процедура

1. Настройте отдельный сервер Windows, используемый для функции восстановления файлов.
2. Установите компонент Data Protection for VMware в системе Windows. При установке примите значения по умолчанию.
3. При конфигурировании компонента Data Protection for VMware в системе Windows используйте следующие имена узлов:
   a. Создайте узел vCenter с именем `VCENTER_FR`.
   b. Создайте узел VMCLI с именем `VMCLI_FR`.
   c. Повторно используйте имя узла центра данных из среды Linux. Например: `DATACENTER`.
   d. Не создавайте узел перемещения данных. Узел перемещения данных не требуется для функции восстановления файлов в этом сценарии.
   e. Создайте следующую новую пару узлов прокси монтирования с именами `REMOTE_FR_MP_WIN` и `REMOTE_FR_MP_LNX`.
4. На странице Восстановление файлов в мастере конфигурирования выберите опцию `Включить восстановление файлов`.
5. Чтобы получить доступ к интерфейсу восстановления файлов, откройте веб-браузер и введите URL, который вам сообщил ваш администратор. Например:

   ```
   https:\\имя_хоста:9081\FileRestoreUI
   ```

   где `имя_хоста` - это имя хоста системы Windows, на котором установлен компонент Data Protection for VMware.

Результаты

В следующем примере показаны взаимосвязи узла прокси на сервере IBM Spectrum Protect:

```
tsm: SERVER>q proxy

Target Node         Agent Node
---------------     ---------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

У дополнительных узлов, созданных, чтобы включить функцию восстановления файлов, есть суффикс _FR.

Изменение опций для операций восстановления файлов

Windows

Чтобы разрешить администраторам конфигурировать обработкой восстановления для операций восстановления файлов и управлять этой обработкой, измените опции в файле frConfig.props.

Об этой задаче

Выполните следующие шаги в системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere.

Процедура

1. Перейдите в каталог, в котором находится файл frConfig.props. Например, откройте командную строку и введите следующую команду:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Откройте файл frConfig.props с помощью текстового редактора в режиме администратора и измените опции нужным вам образом. Используйте информацию в разделе “Опции восстановления файлов”, чтобы определить, какие опции нужно изменить.
3. Сохраните свои изменения и закройте файл frConfig.props.

Результаты

Измененные опции применяются к интерфейсу восстановления файлов IBM Spectrum Protect.

Опции восстановления файлов

Опции frConfig.props управляют конфигурацией, поддержкой и обработкой восстановления для операций восстановления файлов.

enable_contact_info=false | true
Укажите, нужно ли предоставить информацию для контакта с администратором, которую владельцы файлов смогут использовать для получения поддержки.

false
Владельцы файлов не получают информацию для контакта с администратором. Это значение по умолчанию.

true
Владельцы файлов получают информацию для контакта с администратором.

Если вы зададите **enable_contact_info=true**, вы должны ввести информацию в опцию **contact_info**.

enable_filerestore=false | true
Укажите, смогут ли владельцы файлов восстанавливать свои файлы с виртуальной машины с интерфейсом восстановления файлов IBM Spectrum Protect.

false
Владельцы файлов не смогут восстанавливать свои файлы, используя интерфейс восстановления файлов IBM Spectrum Protect. Это значение по умолчанию.

true
Владельцы файлов могут восстанавливать свои файлы, используя интерфейс восстановления файлов IBM Spectrum Protect.

maximum_mount_points=*число_точек_монтирования*
Задайте максимальное число параллельных точек восстановления, доступных для учетной записи пользователя. Минимальное значение - 1 точка восстановления. Максимальное значение - 256 точек монтирования. Значение по умолчанию - 2 точки монтирования.

Совет: Чтобы не разрешить монтировать виртуальную машину несколько раз для выполнения одновременных операций восстановления, задайте для этой опции низкое значение.

mount_session_timeout_minutes=*число_минут*
Задайте время (в минутах), в течение которого точка восстановления и смонтированная точка восстановления могут бездействовать, прежде чем сеанс будет отменен. При отмене точка восстановления будет размонтирована. Максимальное значение - 8 часов (480 минут). Значение по умолчанию - 30 минут.

Совет: Чтобы предотвратить неожиданную отмену сеанса, увеличьте число минут.

restore_info_duration_hours=*число_часов*
Задайте время (в часах), в течение которого информация о последней операции восстановления сохраняется в интерфейсе восстановления файлов IBM Spectrum Protect. Используйте окно операции восстановления для просмотра информации об ошибках и недавно выполненных задачах. Эта информация позволяет найти недавно восстановленные файлы. Максимальное значение - 14 дней (336 часов). Значение по умолчанию - одна неделя (168 часов).

contact_info=*информация об администраторе*
Предоставьте информацию для контакта с администратором, которую владельцы файлов смогут использовать для получения поддержки. Контактная информация появляется в интерфейсе восстановления файлов IBM Spectrum Protect в следующих расположениях:

- Окно для входа в систему
- Панель О программе в меню справки
- Ссылка на информацию о поддержке в сообщениях интерфейса

Можно перезаписать в мастере конфигурирования или блокноте компонента Графический интерфейс Data Protection for VMware vSphere следующие опции:

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

Конфигурирование операций журнала для операций восстановления файлов

Чтобы разрешить администраторам конфигурировать форматирование содержимого и запись в журнал для операций восстановления файлов, а также управлять этой обработкой, измените опции в файле FRLog.config.

Прежде чем начать

Файл FRLog.config генерируется, когда вы в первый раз получаете доступ к интерфейсу восстановления файлов IBM Spectrum Protect.

Об этой задаче

Выполните следующие шаги в системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere.

Процедура

1. Перейдите в каталог, в котором находится файл FRLog.config. Откройте командную строку и введите следующую команду:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```

2. Откройте файл FRLog.config с помощью текстового редактора в режиме администратора и измените опции нужным вам образом. Используйте информацию в разделе “Опции операций журнала восстановления файлов”, чтобы определить, какие опции нужно изменить.
3. Сохраните свои изменения и закройте файл FRLog.config.
4. Перезапустите веб-сервер графического интерфейса:
   a. Щелкните по **Пуск > Панель управления > Администрирование > Службы**.
   b. Щелчкните правой кнопкой мыши по **Служба веб-сервера Data Protection for VMware** и выберите **Перезапустить**.

Результаты

Параметры применяются к содержимому и формату записи информации в журнал для операций восстановления файлов.

Опции операций журнала восстановления файлов

Опции в файле FRLog.config контролируют содержимое и формат записи информации в журнал для операций восстановления файлов.

В файле fr_gui.log есть следующие опции для записи в журнал информации о задачах восстановления файлов:

MAX_LOG_FILES=*число*
Задайте максимальное число файлов fr_gui.log, которые следует сохранять. Значение по умолчанию - 8.

MAX_LOG_FILE_SIZE=*число*
Задайте максимальный размер файла fr_gui.log в КБ. Значение по умолчанию - 8192 КБ.

В файле fr_api.log есть следующие опции записи в журнал информации для служб восстановления файлов. Эти службы - внутренние службы API, связанные с операциями восстановления файлов:

API_MAX_LOG_FILES=*число*
Задайте максимальное число файлов `fr_api.log`, которые следует сохранять. Значение по умолчанию - 8.

API_MAX_LOG_FILE_SIZE=*число*
Задайте максимальный размер файла `fr_api.log` в КБ. Значение по умолчанию - 8192 КБ.

API_LOG_FILE_NAME=*имя_файла_журнала_API*
Укажите имя файла журнала API. Значение по умолчанию: `fr_api.log`.

API_LOG_FILE_LOCATION=*имя_файла_журнала_API*
Укажите расположение файла журнала API. Расположение должно быть задано с использованием обычной обратной черты (/). Расположение по умолчанию: `C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

FR.API.LOG=ON | OFF
Укажите, нужно ли включить запись в журнал для служб восстановления файлов.

- Чтобы включить запись в журнал для служб восстановления файлов, задайте значение ON. Значение по умолчанию: ON.
- Чтобы выключить запись в журнал для служб восстановления файлов, задайте значение OFF.

Чтобы устранить ошибки, с которыми вы можете столкнуться в ходе операции по восстановлению файлов, смотрите раздел Опции трассировки для восстановления файлов. Опции трассировки также заданы в файле `FRLog.config`.

Конфигурирование узла перемещения данных для поддержки тегов

Если на узле перемещения данных включена поддержка тегов, администраторы могут применить теги защиты данных к объектам перечня в VMware vCenter.

Прежде чем начать

Убедитесь, что выполнены следующие требования:

- Сервер VMware vCenter должен быть на уровне Обновление версии 6.0 1 или новее.
- Чтобы компонент Графический интерфейс Data Protection for VMware vSphere правильно функционировал с поддержкой тегов, убедитесь, что при установке графического пользовательского интерфейса выполнены следующие требования:
  - Хотя бы один перенос данных и Графический интерфейс Data Protection for VMware vSphere должны быть установлены на одном и том же сервере. Узел перемещения данных должен быть сконфигурирован таким образом, чтобы идентификационные данные сервера vCenter были сохранены. Можно сохранить идентификационные данные, выполнив мастер конфигурации, чтобы сохранить пароль узла перемещения данных, или с помощью команды **dsmc set password** в командной строке средства перемещения данных.

    При использовании других средств перемещения данных, работающих на виртуальных машинах или физических машинах как дополнительные средства перемещения данных, можно установить их на других серверах. Для поддержки разметки тегами все эти средства перемещения данных надо также сконфигурировать с использованием опции `VMTAGDATAMOVER=yes`. Эти дополнительные средства перемещения данных не требуют Графический интерфейс Data Protection for VMware vSphere установки на том же самом сервере; они все равно будут работать правильно как средства перемещения данных на основе тегов.

– Linux Для функций перемещения данных Linux убедитесь, что вы задали каталог установки функции перемещения данных и совместно используемую библиотеку Java™, `libjvm.so`, в переменной среды `LD_LIBRARY_PATH`. Путь `libjvm.so` используется для поддержки тегов, когда вы включаете опцию `vmtagdatamover` для функции перемещения данных. Инструкции смотрите в разделе Настройка узлов перемещения данных в среде vSphere.

– Linux В операционных системах Linux Графический интерфейс Data Protection for VMware vSphere должен быть установлен с использованием имени пользователя по умолчанию (`tdpvmware`).

– На клиентах UNIX и Linux существующие пароли в файлах `TSM.PWD` переносятся в новое хранилище паролей в том же расположении. Для пользователей root расположение хранилища паролей по умолчанию - `/etc/adsm`. Для пользователей, не являющихся пользователями root, расположение хранилища паролей задано с помощью опции `passworddir`.

  После переноса файл `TSM.PWD` удаляется.

Примечание: Более подробную информацию об использовании полномочий, необходимых для работы с тегами, смотрите в разделе Установка компонентов Data Protection for VMware

Об этой задаче

Можно использовать теги защиты данных, чтобы сконфигурировать политику резервного копирования виртуальных машин в объектах перечня VMware. Эти теги защиты данных представлены как параметры, которые можно изменить в компоненте IBM Spectrum Protect vSphere Client - Модуль plugin.

Процедура

Используйте один из следующих методов:

Опция	Описание
Сконфигурируйте узел перемещения данных при помощи графического пользовательского интерфейса модуля plug-in vSphere	1. В модуле plugin vSphere выберите IBM Spectrum Protect. 2. На вкладке **Конфигурировать** выберите **Средства перемещения данных**. 3. В панели **Добавить средства перемещения данных** выберите в выпадающем меню центр данных. 4. Примите значения по умолчанию или измените значения для параметров **Имя средства перемещения данных**, **Имя хоста средства перемещения данных**, **Пользователь vCenter** и **Пароль vCenter**. 5. Щелкните по **Добавить**, когда закончите работу с параметрами. Дополнительные сведения смотрите в разделе Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere в руководстве по установке Графический интерфейс Data Protection for VMware vSphere.

Опция	Описание
Сконфигурировать *новое* средство перемещения данных для поддержки тегов в Windows или Linux с использованием компонента Графический интерфейс Data Protection for VMware vSphere	1. В системе, где установлен компонент Графический интерфейс Data Protection for VMware vSphere, запустите графический интерфейс, открыв веб-браузер и введя адрес веб-сервера графического интерфейса. Например: `https://<адрес веб-сервера графического интерфейса>:9081/TsmVMwareUI/` 2. Войдите в систему с ID пользователя и паролем vCenter. 3. Перейдите на вкладку **Конфигурация** и выберите действие **Изменить конфигурацию IBM Spectrum Protect**. 4. Перейдите на страницу Узлы перемещения данных в записной книжке конфигурации. 5. Добавьте узел перемещения данных, выполнив следующие шаги: a. Для узла перемещения данных, для которого вы хотите задать поддержку тегов, выберите **Создать службы**. По умолчанию, чтобы включить на узле перемещения данных поддержку тегов, выбрана опция **Узел на основе тегов**. b. Чтобы обозначить узел на основе тега как узел перемещения данных по умолчанию, выберите **Средство перемещения данных по умолчанию**. Узел перемещения данных по умолчанию создает резервные копии всех VM, добавленных в любой контейнер в центре данных, если контейнер уже находятся в защищаемом наборе. Функция перемещения данных по умолчанию также создает резервные копии всех VM в защищаемом наборе, которым не назначен тег `Data Mover`. **Совет:** В системах Linux, если вы выберете новый узел перемещения данных как узел с поддержкой тегов по умолчанию, тогда удалите строку `vmtagdefaultdatamover` из всех других файлов опций перемещения данных, связанных с этим центром данных. c. Щелкните по **ОК**, чтобы сохранить изменения. Опции `vmtagdatamover` и `vmtagdefaultdatamover` (если они заданы) добавляются в файл опций средства перемещения данных (`dsm.opt`).

Опция	Описание
Как сконфигурировать *существующий* узел перемещения данных Windows для поддержки тегов, когда узел находится на том же сервере, что и компонент Графический интерфейс Data Protection for VMware vSphere	1. Выполните шаги 1-3 в предыдущих инструкциях, чтобы сконфигурировать новый узел перемещения данных для поддержки тегов. 2. На странице Узлы перемещения данных выберите **Узел на основе тегов** для узла, для которого вы хотите включить поддержку тегов. 3. **Необязательно:** Чтобы обозначить узел на основе тега как узел перемещения данных по умолчанию, выберите **Средство перемещения данных по умолчанию**.
Как сконфигурировать *существующий* узел перемещения данных Linux для поддержки тегов или существующий узел перемещения данных Windows, который находится не на том же сервере, где находится компонент Графический интерфейс Data Protection for VMware vSphere	1. Добавьте опцию `vmtagdatamover yes` в файл опций средства перемещения данных (`dsm.sys` в случае Linux и `dsm.opt` в случае Windows). 2. **Необязательно:** Чтобы обозначить узел на основе тега как узел перемещения данных по умолчанию, добавьте опцию `vmtagdefaultdatamover yes` или `vmtagdefaultdatamover` *имя_dm* в файл опций средства перемещения данных. **Совет:** В системах Linux, если вы выберете новый узел перемещения данных как узел с поддержкой тегов по умолчанию, тогда удалите строку `vmtagdefaultdatamover` из всех других файлов опций перемещения данных, связанных с этим центром данных.

Результаты

После того, как для узла перемещения данных будет включена поддержка тегов, средство перемещения данных запросит в перечне VMware информацию о тегах, когда запустит резервное копирование. Затем средство перемещения данных создаст резервную копию виртуальных машин в соответствии с заданными тегами защиты данных. Если узел перемещения данных не сконфигурирован для поддержки тегов, все теги защиты данных будут игнорироваться во время операции резервного копирования.

Информация, связанная с данной:

- `Vmtagdatamover`
- `Vmtagdefaultdatamover`
- Конфигурирование политики резервного копирования

Конфигурирование среды для операций полного мгновенного восстановления виртуальной машины

Настройте выделенную сеть iSCSI для операций полного мгновенного восстановления виртуальной машины и мгновенного доступа.

Прежде чем начать

Используйте соответствующую документацию по VMware (ESXi или vSphere), чтобы определить, какие именно шаги нужно выполнить, чтобы сконфигурировать виртуальный коммутатор iSCSI и сети виртуальных машин. Хотя здесь и представлены общие рекомендации, конкретная документация и объяснения того, как добавить виртуальные сети и виртуальные коммутаторы, выходит за пределы документации по продукту. На момент написания данной публикации документация по VMware vSphere ESXi и vCenter 5.5 была доступна в документации по VMware ESXi и vCenter Server 5. В разделе “Сети” содержится информация о добавлении и конфигурировании виртуальных коммутаторов и виртуальных сетей.

Важное замечание: Эти параметры конфигурации помогают настроить среду VMware для выполнения эффективных операций полного мгновенного восстановления виртуальной машины и мгновенного доступа. Однако, поскольку эти параметры относятся к задачам по конфигурированию VMware и пользовательских интерфейсов VMware, вы должны обратиться к соответствующей документации по VMware, чтобы получить подробные, пошаговые инструкции.

Об этой задаче

Эта процедура требует, чтобы на каждом хосте ESXi, использующемся для операций мгновенного восстановления, был адаптер iSCSI. Чтобы настроить адаптер, используйте соответствующую документацию по VMware. На момент написания данной публикации на данном ресурсе VMware vSphere были доступны следующие процедуры.

- Чтобы настроить программный адаптер iSCSI, выполните инструкции процедуры VMware “Сконфигурировать программные адаптеры iSCSI”.
- Чтобы настроить аппаратный адаптер iSCSI, выполните инструкции процедуры VMware “Настройка независимых аппаратных адаптеров iSCSI”.

1. Конфигурирование программы iSCSI на хосте ESXi

Процедура

Эта задача позволяет настроить программу iSCSI для базовой конфигурации.

1. Войдите на хост ESXi, который следует использовать для операций мгновенного восстановления.
2. Следуйте инструкциям в этой статье базы знаний VMware, пока не будет включен адаптер iSCSI: http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect автоматически обнаруживает сервер назначения iSCSI.
3. Убедитесь, что IP-адрес адаптера iSCSI (на хосте ESXi) - это такой же адрес подсети, какой используется средством перемещения данных.
4. Убедитесь, что на хосте ESXi включена лицензия Storage vMotion.

Дальнейшие действия

После настройки программы iSCSI на хосте ESXi установите и сконфигурируйте приложения в системе перемещения данных.

2. Установка и конфигурирование приложений в средстве перемещения данных

Прежде чем начать

Если агент восстановления и средство перемещения данных IBM Spectrum Protect уже установлены и сконфигурированы в системе перемещения данных, начните с шага 3.

Процедура

Эта задача настраивает систему перемещения данных с использованием приложений и параметров для операций мгновенного восстановления.

1. Установите агент восстановления и средство перемещения данных IBM Spectrum Protect в системе перемещения данных.
   В шаге 4 процедуры Установка Data Protection for VMware выберите тип установки **Установить полную функцию перемещения данных для защиты приложений-гостей**.
2. Сконфигурируйте функцию перемещения данных.
   Следуйте инструкциям в разделе "Конфигурирование средства перемещения данных" в документации по клиенту.
3. Задайте IP-адрес сервера iSCSI:
   a. Откройте файл `C:\Program Files\Tivoli\TSM\baclient\dsm.opt` и задайте следующий параметр:

      ```
      VMISCSIServeraddress<IP-адрес сервера iSCSI сетевой карты в системе
      перемещения данных, в которой находятся объекты назначения iSCSI.>
      ```

   Если в системе перемещения данных несколько сетевых карт, то убедитесь, что вы указали нужную сетевую карту для сети iSCSI.

Дальнейшие действия

После настройки системы перемещения данных установите соединение между интерфейсом командной строки агента восстановления и графическим интерфейсом агента восстановления.

3. Настройка соединений агента восстановления

Прежде чем начать

Интерфейс командной строки (command-line interface, CLI) агента восстановления V7.1.x можно рассматривать как API командной строки для графического интерфейса агента восстановления. Интерфейс командной строки агента восстановления можно использовать для взаимодействия с графическим интерфейсом агента восстановления.

Процедура

Эта задача устанавливает соединение между интерфейсом командной строки агента восстановления и графическим интерфейсом агента восстановления.

1. Запустите нтерфейс командной строки агента восстановления в системе перемещения данных.

В меню **Пуск** в Windows выберите **Программы > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > Агент восстановления IBM Spectrum Protect**.

2. В окне командной строки введите следующую команду:

```
RecoveryAgentShell.exe -c set_connection mount_computer <IP-адрес
сетевой карты в системе перемещения данных, в которой находятся объекты назначения iSCSI.>
```

Эта команда устанавливает соединение между интерфейсом командной строки агента восстановления и графическим интерфейсом агента восстановления.

Дальнейшие действия

После установления соединения сконфигурируйте выделенную сеть iSCSI.

4. Конфигурирование выделенной сети iSCSI для хоста ESXi и средства перемещения данных

Прежде чем начать

Прежде чем приступать к этой задаче, ознакомьтесь с этими рекомандациями:

- Используйте для операций мгновенного восстановления выдаленную сеть iSCSI.
- У каждого хоста ESXi, который используется для операций мгновенного восстановления, должна быть вторая физическая сетевая карта. Вторая сетевая карта привязывается к программному адаптеру iSCSI соответствующего хоста ESXi.
- У системы перемещения данных, работающей на виртуальной машине, должна быть вторая сетевая карта. Вторая сетевая карта привязывается к программному адаптеру iSCSI хоста ESXi.
- У каждого хоста ESXi, который используется для операций мгновенного восстановления, должен быть второй склад данных VMware. Этот временный склад данных содержит информацию о конфигурации и данные виртуальной машины, созданной во время операции.

Процедура

Эта задача позволяет настроить выделенную сеть iSCSI для хоста ESXi и для средства перемещения данных, работающего на виртуальной машине.

1. Войдите на хост ESXi, который следует использовать для операций мгновенного восстановления.
2. Настройте виртуальный коммутатор для сети iSCSI.
   Эти шаги используют *vSwitch1* для виртуального коммутатора.
   a. Выберите **Сетевой адаптер VMkernel** для **Тип соединения**.
      Сети iSCSI требуется тип соединения.
   b. Выберите **Создать стандартный коммутатор vSphere** для **Доступ к сети VMkernel**.
   c. Выберите **Метка сети** для опции **Параметры соединения VMkernel**.
      Задайте метку, указывающую на этот коммутатор *vSwitch1*; эта сеть предназначена для вашего трафика iSCSI.
      Например: *VMkernel iSCSI*.
   d. Укажите IP-адрес и маску подсети для *vSwitch1* в **Настройки IP-соединения VMkernel**.
      Не изменяйте значения **Маска подсети** или **Шлюз значения по умолчанию VMkernel**.

e. Задайте порт ядра для работы сети iSCSI.

3. Настройте виртуальный коммутатор для сети виртуальной машины.
   Эти шаги используют *vSwitch0* для виртуального коммутатора.
   a. Выберите **Виртуальная машина** для **Тип соединения**.
   b. Выберите **Создать стандартный коммутатор vSphere** для **Доступ к сети VMkernel**.
   c. Перейдите на вкладку **Свойства группы портов** и выберите **Метка сети**.
   Задайте ту же самую метку, которую вы задали для сети виртуальной машины *vSwitch1*.
   Например: *VMkernel iSCSI*.
4. Привяжите заново созданный адаптер iSCSI к **сетевому адаптеру VMkernel**.
   Выполните инструкции процедуры VMware “Привязка адаптеров iSCSI к адаптерам VMkernel”. На момент написания данной публикации эта процедура была доступна в документации по VMware ESXi и vCenter Server 5.

   Совет: Если при сканировании устройств iSCSI произойдет тайм-аут, сократите число устройств iSCSI, соединяющихся с хостом ESXi. Затем снова просканируйте устройства iSCSI.
5. Убедитесь, что свойства привязки адаптера iSCSI - правильные.
   a. Выберите **Аппаратное обеспечение > Адаптеры хранения** на клиенте VMware vSphere.
   b. Щелкните правой кнопкой мыши по адаптеру iSCSI и выберите **Свойства инициатора iSCSI**. Убедитесь, что существуют следующие свойства привязки:

Таблица 10. Параметры сети iSCSI

Сеть виртуальных машин	Сеть iSCSI
Стандартный коммутатор: *vSwitch0*	**Стандартный коммутатор**: *vSwitch1*
Группа портов виртуальных машин: *Сеть VM*	**Порт VMkernel**: *VMkernel iSCSI* **Совет:** *VMkernel iSCSI* привязывается к **адаптеру VMkernel**: *vmk1*, который находится на **физическом сетевом адаптере**: *vmnic1*.
Физический адаптер: *vmnic0*	**Сетевой адаптер VMkernel**: *vmk1*
	Физический сетевой адаптер: *vmnic1*
	Адаптер виртуальной сети **IP-адрес**: 192.168.42.x (подсеть для сети iSCSI)

Результаты

Выделенная сеть iSCSI готова к операциям полного мгновенного восстановления VM и мгновенного доступа.

Конфигурирование параметров защиты для Data Protection for VMware

Средству перемещения данных Data Protection for VMware, интерфейсу командной строки vmcli и компонентам Графический интерфейс Data Protection for VMware vSphere необходима конфигурация, позволяющая включить защищенное соединение с Сервер IBM Spectrum Protect.

Конфигурирование параметров защиты для соединения функции перемещения данных и узлов VMCLI с Сервер IBM Spectrum Protect

Есть ряд опций конфигурации, относящихся к параметрам защиты Data Protection for VMware для функции перемещения данных и узлов VMCLI при соединении с Сервер IBM Spectrum Protect V7.1.8 или V8.1.2 либо новее. Когда вы принимаете значения по умолчанию для этих опций в прозрачном режиме, эти компоненты конфигурируются для усовершенствованной защиты, и это рекомендуется для большинства случаев использования.

Конфигурирование с использованием параметров защиты по умолчанию (быстрый путь)

Быстрый путь подробно анализирует опции конфигурации, влияющие на защиту соединения функции перемещения данных и узла VMCLI с сервером и на поведение различных случаев использования, когда принимаются значения по умолчанию. Сценарий быстрого пути сводит к минимуму число шагов в процессе конфигурации в конечных точках.

Этот сценарий автоматически получает сертификаты из сервера, когда узел впервые устанавливает соединение, исходя из того, что для параметра **SESSIONSECURITY** Сервер IBM Spectrum Protect задано значение **TRANSITIONAL**, которое является значением по умолчанию при первом соединении. Этому сценарию можно следовать при первом обновлении Сервер IBM Spectrum Protect до V7.1.8 и более новых уровней V7 или до V8.1.2 и более новых уровней V8, а затем при обновлении Data Protection for VMware до этих уровней или наоборот.

Внимание: Этот сценарий нельзя использовать, если сервер IBM Spectrum Protect сконфигурирован для аутентификации LDAP. Если используется LDAP, вы можете вручную импортировать необходимые сертификаты, используя утилиту dsmcert. Дополнительную информацию смотрите в разделе “Конфигурирование без автоматического распределения сертификатов” на стр. 64.

Опции узлов перемещения данных, которые влияют на защиту сеанса

Перечисленные ниже опции dsmc задают параметры защиты для узла перемещения данных. Дополнительную информацию об этих опциях смотрите в документе Справка по опциям клиента.

- `SSLREQUIRED`. Значение по умолчанию, `Default`, включает существующие соединения защиты сеанса с серверами, более ранних версий, чем V7.1.8 или V8.1.2, и автоматически конфигурирует средство перемещения данных Data Protection for VMware для защищенного соединения с сервером V7.1.8 или V8.1.2 либо новее с использованием TLS для аутентификации.
- `SSLACCEPTCERTFROMSERV`. Значение по умолчанию, `Yes`, включает автоматическое принятие самоподписанного открытого сертификата с сервера для функции перемещения данных и автоматически конфигурирует функцию перемещения данных для использования этого сертификата, когда функция перемещения данных соединяется с сервером V7.1.8 или V8.1.2 либо новее.
- `SSL`. Значение по умолчанию, `No`, указывает, что шифрование не используется при передаче данных между функцией перемещения данных и сервером более ранней версии, чем V7.1.8 или V8.1.2. Когда средство перемещения данных соединяется с сервером V7.1.8 или V8.1.2 либо новее, значение по умолчанию, `No`, указывает, что данные объектов не шифруются. Вся остальная информация при взаимодействии средства перемещения данных с сервером шифруется. Значение по умолчанию, `Yes`,

указывает, что TLS используется для шифрования всей информации, включая данные объектов, когда средство перемещения данных взаимодействует с сервером.

- SSLFIPSMODE. Значение по умолчанию, No, указывает, что библиотека TLS, сертифицированная в соответствии с Federal Information Processing Standards (FIPS), не требуется.

Кроме того, перечисленные ниже опции применяются, только если средство перемещения данных использует соединение TLS с сервером более ранней версии, чем V7.1.8 или V8.1.2. Если средство перемещения данных соединяется с более новым сервером, они игнорируются.

- SSLDISABLELEGACYTLS. Значение No указывает, что узел перемещения данных не использует TLS 1.2 для сеансов SSL. Разрешаются соединения по протоколам SSL TLS 1.1 и ниже. Когда функция перемещения данных взаимодействует с Сервер IBM Spectrum Protect, то есть, с V7.1.7 или V8.1.1 или более ранним выпуском, значением по умолчанию будет Нет.
- LANFREESSL. Значение по умолчанию, No, указывает, что функция перемещения данных не использует TLS при взаимодействии с агентом хранения, если сконфигурирована передача данных без локальной сети.
- REPLSSLPORT. Задает адрес порта TCP/IP, который поддерживает TLS, когда средство перемещения данных взаимодействует с сервером репликации назначения.

Опции узлов VMCLI, которые влияют на защиту сеанса

Указанные ниже параметры задают параметры защиты для узла VMCLI. Дополнительную информацию об этих опциях смотрите в разделе Параметры профиля.

- VE_TSM_SSL. Значение по умолчанию, NO, указывает, что шифрование не используется при передаче данных между функцией перемещения данных и сервером более ранней версии, чем V7.1.8 или V8.1.2. Задайте для этого параметра значение YES, если вы хотите использовать TLS для шифрования всей информации при соединении с сервером более ранней версии, чем V7.1.8.
- VE_TSM_SSLACCEPTCERTFROMSERV. Значение по умолчанию, YES, включает автоматическое принятие самоподписанного открытого сертификата с сервера для интерфейса и автоматически конфигурирует интерфейс для использования этого сертификата, когда функция перемещения данных соединяется с сервером V7.1.8 или V8.1.2 либо новее.
- VE_TSM_SSLREQUIRED. Значение по умолчанию, DEFAULT, включает существующие соединения защиты сеанса с серверами, более ранних версий, чем V7.1.8 или V8.1.2, и автоматически конфигурирует интерфейс для защищенного соединения с сервером V7.1.8 или V8.1.2 либо новее с использованием TLS для аутентификации.

Случаи использования для параметров защиты по умолчанию

- Сначала сервер обновляется до V7.1.8, V8.1.2 или новее. Затем Data Protection for VMware обновляется. cEOTCNDE.OBT узел перемещения данных и узлы VMCLI *не* используют связь SSL:
  - Опции защиты для узла перемещения данных и узлов VMCLI изменять не нужно.
  - Когда узлы аутентифицируются с сервером, конфигурация автоматически обновляется для использования TLS.
- Сначала сервер обновляется до V7.1.8, V8.1.2 или новее. Затем Data Protection for VMware обновляется. Существующее средство перемещения данных и узлы VMCLI *используют* связь SSL:

  - Опции защиты для узла перемещения данных и узлов VMCLI изменять не нужно.
  - Связь SSL с существующим публичным сертификатом сервера продолжает использоваться.
  - Связь SSL автоматически усовершенствуется так, чтобы использовать тот уровень TLS, который требуется серверу.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2 или новее. Затем сервер обновляется позднее. cEOTCNDE.OBT узел перемещения данных и узлы VMCLI *не* используют связь SSL:
  - Опции защиты для узла перемещения данных и узлов VMCLI изменять не нужно.
  - Существующий протокол аутентификации по-прежнему используется серверами на уровнях до V7.1.8 или V8.1.2.
  - Когда узлы аутентифицируются с сервером, конфигурация автоматически обновляется для использования TLS, после того, как сервер будет обновлен до V7.1.8, V8.1.2 или новее.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2 или новее. Затем сервер обновляется позднее. Существующее средство перемещения данных и узлы VMCLI *используют* связь SSL:
  - Опции защиты для узла перемещения данных и узлов VMCLI изменять не нужно.
  - Связь SSL с существующим публичным сертификатом сервера продолжает использоваться с серверами на уровнях до V7.1.8 или V8.1.2.
  - Связь SSL автоматически усовершенствуется так, чтобы использовать тот уровень TLS, который требуется серверу, после того, как сервер будет обновлен до V7.1.8, V8.1.2 или новее.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2 или новее. Затем средство перемещения данных и узлы VMCLI соединяются с несколькими серверами. Серверы обновляются в разное время:
  - Опции защиты для узла перемещения данных и узлов VMCLI изменять не нужно.
  - Средство перемещения данных и узлы VMCLI используют существующую аутентификацию и протокол защиты сеанса с серверами более ранних версий, чем версия 7.1.8 или 8.1.2, и автоматически обновляется для использования аутентификации TLS при первоначальном соединении с сервером версии 7.1.8 или 8.1.2 либо новее. Защитой сеанса управляют на каждом сервере.
- При новой установке клиента сервер относится к версии 7.1.8 или 8.1.2 либо новее:
  - Сконфигурируйте Data Protection for VMware в соответствии с новой установкой.
  - Значения по умолчанию для опций защиты автоматически конфигурируют средство перемещения данных и узлы VMCLI для аутентификации сеансов, зашифрованных с использованием TLS.
  - Задайте для параметра SSL значение `Yes`, если требуется шифрование всех передаваемых данных между клиентом и сервером.
- При новой установке клиента сервер относится к версии, более ранней, чем V7.1.8 или V8.1.2:
  - Сконфигурируйте клиент в соответствии с новой установкой клиента.
  - Примите значения по умолчанию для параметров защиты сеанса клиента, если вам не требуется шифрование SSL для всех передач данных.
    - Протокол аутентификации без поддержки SSL используется, пока сервер не будет обновлен до V7.1.8 или V8.1.2 либо новее.

– Задайте для параметра SSL значение Yes, если требуется шифрование всех передаваемых данных между функцией перемещения данных и сервером, и перейдите к конфигурированию поддержки SSL вручную.
  - Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
  - Связь SSL автоматически усовершенствуется так, чтобы использовать тот уровень TLS, который требуется серверу, после того, как сервер будет обновлен до V7.1.8, V8.1.2 или новее.

Конфигурирование без автоматического распределения сертификатов

Этот сценарий подробно анализирует опции конфигурации, влияющие на защиту соединения функции перемещения данных и узлов VMCLI, если автоматическое распределение сертификатов с сервера не приемлемо. Например, автоматическое распределение сертификатов с сервера будет неприемлемым, если сервер сконфигурирован для использования аутентификации LDAP или если требуется, чтобы сертификаты были подписаны центром сертификации (certificate authority, CA).

Опции, влияющие на защиту сеансов

Опции для параметров защиты такие же, как описано в разделе “Конфигурирование с использованием параметров защиты по умолчанию (быстрый путь)” на стр. 61, с тем исключением, что нужно задать для опции SSLACCEPTCERTFROMSERV значение No, чтобы узел перемещения данных не принимал автоматически самоподписанный общедоступный сертификат с сервера, когда узел впервые соединяется с сервером V7.1.8 или V8.1.2 либо новее.

Случаи использования при конфигурировании узлов средства перемещения данных без автоматического распределения сертификатов

Если автоматическое распределение сертификатов является невозможным или нежелательным, используйте утилиту dsmcert для импорта сертификата. Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA. CA может относиться к такой компании, как VeriSign или Thawte, или это должен быть внутренний сертификат, хранящийся в вашей компании.

Если узлы перемещения данных и VMCLI находятся на том же компьютере, требуется только один сертификат. Если узлы находятся на отдельных компьютерах, то сертификат требуется для каждого компьютера.

- Сначала сервер обновляется до V7.1.8 или V8.1.2. Затем Data Protection for VMware обновляется. Существующие узлы средства перемещения данных *не* используют связь SSL:
  – Задайте для опции SSLACCEPTCERTFROMSERV значение No.
  – Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
- Сначала сервер обновляется до V7.1.8 или V8.1.2. Затем Data Protection for VMware обновляется. Существующие узлы средства перемещения данных *используют* связь SSL:

  - Опции защиты для узла перемещения данных изменять не нужно. Если у узлов уже есть сертификат сервера для связи SSL, то опция SSLACCEPTCERTFROMSERV не применяется.
  - Связь SSL с существующим публичным сертификатом сервера продолжает использоваться.
  - Связь SSL автоматически усовершенствуется так, чтобы использовать тот уровень TLS, который требуется серверу.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2. Затем сервер обновляется позднее. Существующие узлы средства перемещения данных *не* используют связь SSL:
  - Задайте для опции SSLACCEPTCERTFROMSERV значение No.
  - Существующий протокол аутентификации по-прежнему используется серверами на уровнях до V7.1.8 или V8.1.2.
  - Прежде чем узлы средства перемещения данных соединятся с сервером V7.1.8, V8.1.2 или новее:
    - Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2. Затем сервер обновляется позднее. Существующие узлы средства перемещения данных *используют* связь SSL
  - Опции защиты для узла перемещения данных изменять не нужно. Если у узлов уже есть сертификат сервера для связи SSL, то опция SSLACCEPTCERTFROMSERV не применяется.
  - Связь SSL с существующим публичным сертификатом сервера продолжает использоваться с серверами на уровнях до V7.1.8 или V8.1.2.
  - Связь SSL автоматически усовершенствуется так, чтобы использовать тот уровень TLS, который требуется серверу, после того, как сервер будет обновлен до V7.1.8, V8.1.2 или новее.
- Сначала Data Protection for VMware обновляется до V7.1.8 или V8.1.2. Затем узлы средства перемещения данных соединяются с несколькими серверами. Серверы обновляются в разное время:
  - Задайте для опции SSLACCEPTCERTFROMSERV значение No.
  - Существующий протокол аутентификации по-прежнему используется серверами на уровнях до V7.1.8 или V8.1.2.
  - Прежде чем узлы перемещения данных соединятся с сервером V7.1.8 или V8.1.2 либо новее или если требуется связь SSL на любом уровне сервера:
    - Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
  - Узлы перемещения данных используют существующую аутентификацию и протокол защиты сеанса с серверами более ранних версий, чем версия 7.1.8 или 8.1.2, и автоматически обновляется для использования аутентификации TLS при первоначальном соединении с сервером версии 7.1.8 или 8.1.2 либо новее. Защитой сеанса управляют на каждом сервере.
- При новой установке Data Protection for VMware сервер относится к версии 7.1.8 или 8.1.2 либо новее:
  - Сконфигурируйте Data Protection for VMware в соответствии с новой установкой.
  - Задайте для опции SSLACCEPTCERTFROMSERV значение No.

  - Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
  - Задайте для параметра SSL значение `Yes`, если требуется шифрование всех передаваемых данных между функцией перемещения данных и сервером.
- При новой установке Data Protection for VMware сервер относится к версии, более ранней, чем V7.1.8 или V8.1.2, сеансы с шифрованием SSL *требуются*:
  - Сконфигурируйте Data Protection for VMware в соответствии с новой установкой.
  - Задайте для параметра SSL значение `Yes`.
  - Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.
- При новой установке Data Protection for VMware сервер относится к версии, более ранней, чем V7.1.8 или V8.1.2, сеансы с шифрованием SSL *не* требуются:
  - Сконфигурируйте Data Protection for VMware в соответствии с новой установкой.
  - Задайте для опции `SSLACCEPTCERTFROMSERV` значение `No`.
    - Протокол аутентификации без поддержки SSL используется, пока сервер не будет обновлен до V7.1.8 или V8.1.2 либо новее.
  - Прежде чем узлы средства перемещения данных соединятся с сервером V7.1.8, V8.1.2 или новее:
    - Получите нужный сертификат от Сервер IBM Spectrum Protect или от CA и используйте утилиту dsmcert для импорта сертификата. Инструкции по конфигурированию смотрите в разделе Конфигурирование связи между клиентом и сервером Tivoli Storage Manager с помощью Secure Sockets Layer.

Конфигурирование связи Графический интерфейс Data Protection for VMware vSphere с использованием Transport Layer Security

Компонент Графический интерфейс Data Protection for VMware vSphere использует протокол Transport Layer Security (TLS), чтобы обеспечить защищенную связь с веб-браузерами, сервером VMware vCenter и (необязательно) Сервер IBM Spectrum Protect.

Об этой задаче

Для взаимодействий с веб-браузерами и с сервером VMware VCenter протокол TLS включается всегда. При установке компонента Data Protection for VMware генерируется самоподписанный цифровой сертификат TLS, который затем используется для соединения.

Также для взаимодействия с веб-браузерами можно использовать сертификат, подписанный центром сертификации (certificate authority, CA). Data Protection for VMware Чтобы узнать, как использовать сертификат от CA, смотрите раздел Использование сертификата третьей стороны для сеансов веб-браузера.

В случае взаимодействия с Сервер IBM Spectrum Protect использование протокола TLS зависит от версии сервера.

Если вы используете сервер Сервер IBM Spectrum Protect V8.1.1 или более ранний
Использование протокола TLS для взаимодействий с сервером не является обязательным. Вы можете вручную включить для Графический интерфейс

Data Protection for VMware vSphere возможность взаимодействовать с сервером при помощи протокола TLS, создав или обновив склад доверенных сертификатов и импортировав сертификат, как описано в разделе “Обеспечение защищенного обмена информацией с сервером IBM Spectrum Protect”

Если вы используете сервер Сервер IBM Spectrum Protect V7.1.8, V8.1.2 или новее
Требуется протокол TLS. В большинстве случаев склад доверенных сертификатов создается автоматически при первом использовании на основе параметров защиты по умолчанию, описанных в разделе “Конфигурирование с использованием параметров защиты по умолчанию (быстрый путь)” на стр. 61. Однако в некоторых сценариях вам может потребоваться вручную создать склад доверенных сертификатов. .

Важное замечание: Сценарий быстрого пути автоматически получает сертификаты, когда Графический интерфейс Data Protection for VMware vSphere впервые взаимодействует с сервером, исходя из того, что для параметра **SESSIONSECURITY** Сервер IBM Spectrum Protect задано значение **TRANSITIONAL**, которое является значением по умолчанию при первом соединении. После соединения графического интерфейса с сервером параметру **SESSIONSECURITY** присваивается значение **STRICT**. Поскольку графический интерфейс использует для соединения с сервером ID администратора сервера, то, если другой объект использует этот ID для соединения, в графическом интерфейсе при попытке соединиться с сервером появятся сообщения об ошибках. Чтобы устранить эту проблему, снова задайте для параметра **SESSIONSECURITY** значение **TRANSITIONAL**.

Обеспечение защищенного обмена информацией с сервером IBM Spectrum Protect

Если вы используете сервер IBM Spectrum Protect версии 7.1.7 или более ранний либо V8.1.2 или более ранний, соединение с сервером с использованием протокола TLS является необязательным, и, если вы хотите включить Графический интерфейс Data Protection for VMware vSphere для взаимодействия с сервером с использованием протокола, вы должны включить связь вручную.

Прежде чем начать

Получите копию сертификата от администратора сервера.

Об этой задаче

Если вы используете сервер версии 7.1.8 или 8.1.2 либо новее, протокол TLS является обязательным и при первом использовании автоматически создается склад доверенных сертификатов с сертификатом с и использованием параметров защиты по умолчанию, описанных в разделе “Конфигурирование с использованием параметров защиты по умолчанию (быстрый путь)” на стр. 61. Однако в некоторых сценариях вам может потребоваться вручную создать склад доверенных сертификатов и сконфигурировать Графический интерфейс Data Protection for VMware vSphere, как описано в данной теме.

В описанной ниже процедуре используется ключ Java™ и инструмент управления сертификатами **keytool**.

В операционных системах Linux этот инструмент находится в каталоге `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

В операционных системах Microsoft Windows этот инструмент находится в каталоге `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre\bin`.

При вводе команды **keytool**, возможно, потребуется указать полный путь.

Процедура

1. Из командной строки измените каталог на расположение базы доверенных сертификатов:
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - В Windows: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. Создайте склад доверенных сертификатов и импортируйте сертификат с помощью следующей команды:

   ```
   keytool -importcert -alias my-cert -file cert.pem -keystore
   tsm-ve-truststore.jks -storepass пароль
   ```

   Где:

   -alias *my-cert*
   : Уникальный алиас, определяющий сертификат в базе доверенных сертификатов.

   -file *cert.pem*
   : Файл, содержащий самоподписанный сертификат сервера или корневой сертификат CA.

   -storepass *пароль*
   : Пароль склада ключей. Убедитесь, что вы запомнили этот пароль для последующего использования.
3. Запустите компонент Графический интерфейс Data Protection for VMware vSphere и перейдите в окно Конфигурация.
   - Если вы создаете начальную конфигурацию, щелкните по **Задачи > Запустить мастер конфигурирования IBM Spectrum Protect** и перейдите на страницу Идентификационные данные сервера.
   - Если вы изменяете существующую конфигурацию, щелкните по **Задачи > Изменить конфигурацию IBM Spectrum Protect** и перейдите на страницу Идентификационные данные сервера.
4. Введите номер порта в поле **Порт администратора IBM Spectrum Protect**. Это порт сервера, который позволяет осуществлять административные соединения с использованием SSL или TLS.
5. Выберите **Использовать шифрованную связь на порту администрирования**.
6. Если вы хотите использовать этот параметр для сеансов графического интерфейса в будущем, выберите **Сохранить ID администратора, пароль и параметры порта**.
7. Щелкните по **ОК**, чтобы применить изменения.

Использование сертификата от центра сертификации

Чтобы использовать сертификат, подписанный центром сертификации, то нужно выполнить несколько шагов.

Об этой задаче

В перечисленных ниже процедурах используется стандартный ключ и инструмент управления сертификатами, который называется **keytool**.

В операционных системах Linux этот инструмент находится в каталоге `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

В операционных системах Microsoft Windows этот инструмент находится в каталоге `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre`.

При запуске **keytool** из командной строки вам, возможно, придется указать полный путь.

Процедура

1. Получите доступ к складу ключей.
2. Создайте требование подписи сертификата (certificate signing request, CSR).
3. Отправьте требование подписи сертификата в центр сертификации для подписи.
4. Получите подписанный сертификат в компонент Графический интерфейс Data Protection for VMware vSphere.

Получение доступа к складу ключей:

Сертификаты хранятся в складе ключей Java. Содержимое склада ключей защищено паролем. Чтобы управлять сертификатами в складе ключей, нужно получить доступ к складу ключей.

Об этой задаче

Подписанный сертификат по умолчанию и пароль склада ключей генерируются при установке, поэтому вам вряд ли будет известен исходный пароль.

Выполните следующую процедуру, чтобы зменить исходный склад ключей на новый склад ключей и новый самоподписанный сертификат. Новый склад ключей защищен паролем по вашему выбору.

Если вы уже знаете пароль склада ключей, пропустите эту процедуру.

Процедура

1. Остановите службу Графический интерфейс Data Protection for VMware vSphere.
2. Из командной строки измените каталог на расположение склада ключей.
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - В Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
3. Создайте резервную копию файла склада ключей (`key.jks`), переименовав его или переместив в другое расположение.
4. Создайте новый склад ключей и новый самоподписанный сертификат, введя следующую команду:

```
keytool -genkeypair -alias vekey -dname
CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity дни -keystore
key.jks -storepass пароль -keypass пароль
```

Где:

-dname CN=*полное_имя_домена***,OU=Tivoli_Storage_Manager_for_VMware,O=IBM**
полное_имя_домена - это имя DNS или полное имя домена компьютера, на котором установлен компонент Графический интерфейс Data Protection for VMware vSphere.

-validity *дни*
Срок действия сертификата.

-storepass *пароль*
Пароль склада ключей. Убедитесь, что вы запомнили этот пароль для последующего использования.

-keypass *пароль*
Пароль секретного ключа для сертификата. Этот пароль должен соответствовать паролю склада ключей.

5. Закодируйте пароль склада ключей, используя инструмент **securityUtility**. Введите следующую команду
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - В Windows: `C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

   Введите свой пароль склада ключей, когда вас об этом попросят, а затем сохраните выходную информацию (например, скопируйте ее в буфер обмена).
6. Откройте файл `bootstrap.properties` в редакторе и задайте для свойства `veProfile.keystore.pswd` закодированное значение из предыдущего шага. Файл `bootstrap.properties` находится в следующем расположении:
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
   - В Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\`
7. Запустите службу Графический интерфейс Data Protection for VMware vSphere.

Ссылки, связанные с данной:

“Запуск программы и служб для Data Protection for VMware” на стр. 92

Создание требования подписи сертификата:

После получения доступа к складу ключей нужно создать требование подписи сертификата (certificate signing request, CSR).

Процедура

Чтобы создать CSR, выполните следующие шаги:

1. Из командной строки измените каталог на расположение склада ключей.
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - В Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Создайте новый сертификат, введя следующую команду:

```
keytool -genkeypair -alias мой_ключ -dname
CN=полное_имя_домена,OU=подразделение,O=организация -keyalg RSA -sigalg SHA256withRSA
-keysize 2048 -validity дни -keystore key.jks -storepass
пароль -keypass пароль
```

Где:

-alias *мой_ключ*
: *мой_ключ* - это уникальный алиас, идентифицирующий сертификат в складе ключей. Он переименовывается при получении подписанного сертификата.

-dname CN=*полное_имя_домена***,OU=***подразделение***,O=***организация*
: *полное_имя_домена* - это имя DNS или полное имя домена компьютера, на котором установлен компонент Графический интерфейс Data Protection for VMware vSphere.

  подразделение и *организация* - это информация об организации, которую требуют задать ваши правила политики или центр сертификации.

-validity *дни*
: Срок действия сертификата.

-storepass *пароль*
: Пароль склада ключей. Если вы не знаете пароль склада ключей или забыли его, смотрите раздел “Получение доступа к складу ключей” на стр. 69.

-keypass *пароль*
: Пароль секретного ключа для сертификата. Этот пароль должен соответствовать паролю склада ключей.

3. Создайте CSR, введя следующую команду:

   ```
   keytool -certreq -alias мой_ключ -file требование_сертификата.pem -keystore key.jks
   ```

   Где:

   -alias *мой_ключ*
   : Алиас сертификат из предыдущего шага.

   -file *требование_сертификата.pem*
   : Файл, в котором нужно сохранить требование подписи сертификата.

Отправка требования подписи сертификата в центр сертификации:

После создания требования подписи сертификата (`certreq.pem`) вы должны отправить его в центр сертификации для получения подписи. Следуйте конкретным инструкциям центра сертификации.

Получение подписанного сертификата:

Почле получения подписанного сертификата от центра сертификации (certificate authority, CA) нужно получить сертификат в склад ключей.

Процедура

Чтобы получить подписанный сертификат, выполните следующие шаги:

1. Из командной строки измените каталог на расположение склада ключей.
   - В Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`

- В Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`

2. Скопируйте в этот каталог файлы, полученные от CA. Эти файлы включают в себя корневой сертификат CA, промежуточные сертификаты CA (если они есть) и подписанные сертификаты для компонента Графический интерфейс Data Protection for VMware vSphere.
3. Остановите службу Графический интерфейс Data Protection for VMware vSphere.
4. Создайте резервную копию файла склада ключей (`key.jks`), скопировав его под другим именем или в другое расположение.
5. Импортируйте промежуточный сертификат CA (если он есть) с помощью следующей команды. Когда вас спросят, нужно ли доверять сертификатам, ответьте *yes*. Повторите этот шаг для нескольких промежуточных сертификатов CA, если это потребуется.

   ```
   keytool -importcert -alias ca-intermediate -file intermediate.pem
   -keystore key.jks -storepass пароль
   ```

   Где:

   -alias *ca-intermediate*
   : Уникальный алиас, определяющий сертификат на складе ключей. У каждого промежуточного сертификата должен быть уникальный алиас.

   -file *intermediate.pem*
   : Файл промежуточного сертификата, полученный от CA.

   -storepass *пароль*
   : Пароль склада ключей.

6. Импортируйте корневой сертификат CA, введя следующую команду. Когда вас спросят, нужно ли доверять этому сертификату, ответьте *yes*.

   ```
   keytool -importcert -alias ca-root -file root.pem -keystore
   key.jks -storepass пароль
   ```

   Где:

   -alias *ca-root*
   : Уникальный алиас, определяющий сертификат на складе ключей.

   -file *root.pem*
   : Файл корневого сертификата, полученный от CA.

   -storepass *пароль*
   : Пароль склада ключей.

7. Импортируйте подписанный сертификат, введя следующую команду:

   ```
   keytool -importcert -alias mykey -file signedcert.pem -keystore
   key.jks -storepass пароль
   ```

   Где:

   -alias *мой_ключ*
   : Алиас подписанного сертификата. Алиас должен быть таким же, какой использовался, когда вы сгенерировали требование подписи сертификата (certificate signing request, CSR).

   -file *signedcert.pem*
   : Файл подписанного сертификата, полученный от CA.

   -storepass *пароль*
   : Пароль склада ключей.

8. Удалите существующий сертификат, содержащий алиас `vekey`:

```
keytool -delete -alias vekey -keystore key.jks -storepass пароль
```

Где `-storepass` *пароль* - это пароль для склада ключей.

9. Переименуйте подписанный сертификат в `vekey`:

```
keytool -changealias -alias мой_ключ -destalias vekey -keystore
key.jks -storepass пароль
```

Где:

`-alias` *mykey*
Алиас подписанного сертификата.

`-storepass` *пароль*
Пароль склада ключей.

10. Запустите службу Графический интерфейс Data Protection for VMware vSphere.

Ссылки, связанные с данной:

“Запуск программы и служб для Data Protection for VMware” на стр. 92

Требования к полномочиям пользователя сервера VMware vCenter

Для выполнения операций Data Protection for VMware требуются некоторые особые полномочия сервера VMware vCenter.

Полномочия сервера vCenter, необходимые для защиты центров данных VMware с представлением веб-браузера для Графический интерфейс Data Protection for VMware vSphere

У ID пользователя сервера vCenter, который входит в представление браузера для Графический интерфейс Data Protection for VMware vSphere,

должны быть достаточные полномочия VMware, чтобы просматривать содержимое центра данных, управляемого графическим интерфейсом.

Например, среда VMware vSphere содержит пять центров данных. У пользователя “jenn” достаточно полномочий только для двух из этих центров данных. Поэтому в представлениях пользователь “jenn” увидит только два из этих центров данных, для доступа к которым у него есть достаточные полномочия. Другие три центра данных (на доступ к которым у пользователя “jenn” нет полномочий) будут не видны пользователю “jenn”.

Сервер VMware vCenter задает ряд полномочий в совокупности в виде роли. Роль применяется к объекту для указанного пользователя или группы, чтобы создать полномочия. Вы должны создать роль с набором полномочий с веб-клиента VMware vSphere. Чтобы создать роль сервера vCenter для операций резервного копирования и восстановления, используйте функцию **Добавить роль** на клиенте VMware vSphere.

Если вы хотите распространить эти полномочия на все центры данных в пределах vCenter, задайте сервер vCenter и включите переключатель `распространять на дочерние`. Или вы можете ограничить разрешения, если назначите роль для нужных центров данных, только при включенном переключателе `распространять на дочерние`. Принудительное применение для графического интерфейса браузера находится на уровне центра данных.

В следующем примере показано, как управлять доступом к центрам данных для двух групп пользователей VMware. Сначала создайте роль, у которой будут все полномочия, указанные в technote 7047438. Набор полномочий в этом примере указан

ролью “TDPVMwareManage”. Группе 1 требуется доступ, чтобы управлять виртуальными машинами для центров данных `Primary1_DC` и `Primary2_DC`. Группе 2 требуется доступ, чтобы управлять виртуальными машинами для центров данных `Secondary1_DC` и `Secondary2_DC`.

Назначьте группе 1 роль “TDPVMwareManage” для центров данных `Primary1_DC` и `Primary2_DC`. Назначьте группе 2 роль “TDPVMwareManage” для центров данных `Secondary1_DC` и `Secondary2_DC`.

Пользователи в каждой группе пользователей VMware смогут использовать графический интерфейс Data Protection for VMware для управления виртуальными машинами только в соответствующих центрах данных.

Совет: При создании роли рассмотрите возможность добавить в роль дополнительные полномочия, которые могут потом понадобиться для выполнения других задач с объектами.

Полномочия сервера vCenter, необходимые для использования средства перемещения данных

Средству перемещения данных IBM Spectrum Protect, установленное на сервере резервного копирования vStorage Backup (узел перемещения данных), требуются опции `VMCUser` и `VMCPw`. Опция `VMCUser` задает ID пользователя сервера vCenter или ESX, который вам нужен, чтобы производить резервное копирование, восстановление или запрос. Необходимые полномочия, назначенные этому ID пользователя (`VMCUser`), гарантируют, что клиент сможет выполнять операции на виртуальной машине и в среде VMware. У этого ID пользователя должны быть полномочия VMware, описанные в указанной выше технической записке.

Чтобы создать роль сервера vCenter для операций резервного копирования и восстановления, используйте функцию **Добавить роль** на клиенте VMware vSphere. При добавлении полномочий для этого ID пользователя (`VMCUser`) вы должны выбрать опцию `распространять на дочерние`. Кроме того, рассмотрите возможность добавления в эту роль других полномочий для задач помимо резервного копирования и восстановления. Для опции `VMCUser` принудительное применение осуществляется для объекта высшего уровня.

Полномочия сервера vCenter, необходимые для защиты центров данных VMware с представлением IBM Spectrum Protect vSphere Client - Модуль plugin для Графический интерфейс Data Protection for VMware vSphere

Компоненту IBM Spectrum Protect vSphere Client - Модуль plugin требуется набор полномочий отдельно от полномочий, необходимых для входа в графический интерфейс.

При установке для компонента IBM Spectrum Protect vSphere Client - Модуль plugin создаются следующие пользовательские полномочия:

- **Центр данных > IBM Data Protection**
- **Глобальные > Сконфигурировать IBM Data Protection**

Пользовательские полномочия, которые необходимы для компонента IBM Spectrum Protect vSphere Client - Модуль plugin, регистрируются как отдельное расширение. Ключ расширения полномочий - `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Эти полномочия позволяют администратору VMware включать и выключать доступ к содержимому компонента IBM Spectrum Protect vSphere Client - Модуль plugin. Получать доступ к содержимому IBM Spectrum Protect vSphere Client - Модуль plugin могут только пользователи с этими пользовательскими полномочиями для необходимого объекта VMware. Для каждого сервера vCenter регистрируется по одному компоненту IBM Spectrum Protect vSphere Client - Модуль plugin, и он совместно используется всеми хостами графического интерфейса, сконфигурированными для поддержки сервера vCenter.

На веб-клиенте VMware vSphere нужно создать роль для пользователей, которые смогут выполнять функции защиты данных для виртуальных машин, используя компонент IBM Spectrum Protect vSphere Client - Модуль plugin. Для этой роли, в дополнение к стандартным полномочиям роли администратора виртуальных машин, необходимым веб-клиенту, нужно задать полномочия **Центр данных > IBM Data Protection**. Для каждого центра данных назначьте эту роль каждому пользователю или группе пользователей, пользователям которой вы хотите предоставить разрешение на управление виртуальными машинами.

Полномочия **Глобальный > IBM Data Protection** необходимы пользователю на уровне vCenter. Это полномочие позволяет пользователю управлять, изменять или стирать соединение между сервером vCenter и веб-сервером Графический интерфейс Data Protection for VMware vSphere. Назначьте эти полномочия администраторам, которые знакомы с компонентом Графический интерфейс Data Protection for VMware vSphere, который защищает соответствующий сервер vCenter. Управляйте соединениями компонента IBM Spectrum Protect vSphere Client - Модуль plugin на странице Соединения расширения.

В следующем примере показано, как управлять доступом к центрам данных для двух групп пользователей. Группе 1 требуется доступ, чтобы управлять виртуальными машинами для центров данных `NewYork _DC` и `Boston_DC`. Группе 2 требуется доступ, чтобы управлять виртуальными машинами для центров данных `LosAngeles_DC` и `SanFranciso_DC`.

На клиенте VMware vSphere создайте, например, роль “IBMDataProtectManage”, назначьте стандартные полномочия роли администратора виртуальных машин, а также полномочия **Центр данных > IBM Data Protection**.

Назначьте группе 1 роль “IBMDataProtectManage” для центров данных `NewYork_DC` и `Boston_DC`. Назначьте группе 2 роль “IBMDataProtectManage” для центров данных `LosAngeles_DC` и `SanFranciso_DC`.

Пользователи в каждой группе смогут использовать компонент IBM Spectrum Protect vSphere Client - Модуль plugin на веб-клиенте vSphere для управления виртуальными машинами только в соответствующих центрах данных.

Проблемы, связанные с недостаточными полномочиями

Если у пользователя веб-браузера нет достаточных полномочий ни для какого центра обработки данных, доступ к представлению блокируется. Вместо этого генерируется сообщение об ошибке GVM2013E, чтобы указать, что пользователь не авторизован для получения доступа ни к каким управляемым центрам данных из-за недостатка разрешений. Также есть другие новые сообщения, которые информируют пользователей о проблемах из-за недостаточных разрешений. Чтобы устранить проблемы, связанные с разрешениями, убедитесь, что роль пользователя задана, как рассказывается в предыдущих разделах. У роли пользователя должны быть все полномочия, указанные в необходимых полномочиях для ID пользователя сервера

vCenter и таблицы перемещения данных, и эти полномочия должны быть применены на уровне центра данных с включенным переключателем `распространять на дочерние`.

Если у пользователя компонента IBM Spectrum Protect vSphere Client - Модуль plugin нет достаточных полномочий на доступ к центру данных, функции защиты данных для этого центра данных и его содержимое станут недоступны в расширении.

Если у ID пользователя IBM Spectrum Protect (заданного опцией `VMCUser`) недостаточно полномочий для выполнения операции резервного копирования и восстановления, появится следующее сообщение:

```
ANS9365E Ошибка API VMware vStorage.
"Отказано в разрешении на выполнение этой операции."
```

Если у ID пользователя IBM Spectrum Protect недостаточно полномочий на просмотр компьютера, появятся следующие сообщения:

```
Команда резервного копирования виртуальных машин запущена.  Всего виртуальных машин
для обработки: 1
ANS4155E Не удалось найти виртуальную машину 'tango' на сервере VMware.
ANS4148E Полное резервное копирование виртуальной машины 'foxtrot' завершилось
         неудачно с кодом возврата 4390
```

Более подробную информацию об использовании полномочий смотрите в замечании в разделе **Полномочия сервера vCenter, необходимые для графического интерфейса Data Protection for VMware vSphere и средства перемещения данных**.

Чтобы получить информацию журнала через сервер VMware Virtual Center для устранения проблем с разрешениями, выполните следующие шаги:

1. В окне Параметры сервера vCenter выберите **Опции записи в журнал** и задайте для опции "**Запись в журнал vCenter** значение **Trivia (Trivia)**.
2. Воспроизведите ошибку разрешений.
3. Переустановите для опции **Запись в журнал vCenter** ее предыдущее значение, чтобы запретитмь запись лишней информации журнала.
4. В окне Системные журналы найдите самый последний журнал сервера vCenter (`vpxd-`*`wxyz`*`.log`) и найдите строку `NoPermission`. Например:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Ошибка вызова:
   Сеанс vim.VirtualMachine.createSnapshot: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Сгенерировано: vim.fault.NoPermission
   ```

   Это сообщение журнала указывает, что у ID пользователя нет достаточных полномочий на создание снимка (`createSnapshot`).

Роли пользователей Графический интерфейс Data Protection for VMware vSphere

Доступность функций компонента Графический интерфейс Data Protection for VMware vSphere основана на уровне авторизации, назначенном ID вашего администратора IBM Spectrum Protect.

ID администратора должен совпадать с именем узла. В более ранних выпусках продукта команда **`REGISTER NODE`** автоматически создавала ID административного пользователя, имя которого совпадало с именем узла. Начиная с IBM Spectrum Protect V8.1, команда **`REGISTER NODE`** не создает автоматически ID пользователя-администратора, соответствующий имени узла.

При регистрации нового узла администратор сервера IBM Spectrum Protect должен задать параметр `userid` с помощью команды сервера **`REGISTER NODE`**.

```
REGISTER NODE имя_узла пароль userid=id_пользователя
```

Где имя узла и ID административного пользователя должны иметь одно и то же значение. Например:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

По умолчанию у узла есть полномочия владельца клиента.

Задачи, которые можно выполнить с помощью компонента Графический интерфейс Data Protection for VMware vSphere, основаны на классе полномочий, назначенных для ID администратора.

Если у ID администратора нет полномочий Неограниченная политика домена, то вы не можете регистрировать новые узлы или задавать их взаимосвязи прокси на сервере IBM Spectrum Protect. Если вы не введете ID администратора, то будет создан сценарий макрокоманд, чтобы вы могли работать на сервере IBM Spectrum Protect.

ID администратора IBM Spectrum Protect требуется при конфигурировании компонента Графический интерфейс Data Protection for VMware vSphere. В следующей таблице описаны функции, доступные в зависимости от класса полномочий, назначенного этому ID:

- Да означает, что функция доступна для роли пользователя.
- Нет означает, что функция недоступна для роли пользователя.

Чтобы посмотреть свою текущую роль модуля Графический интерфейс Data Protection for VMware vSphere, поместите указатель мыши на свой ID пользователя в панели навигации.

Таблица 11. Доступные функции, основанные на требованиях к полномочиям для ID администратора IBM Spectrum Protect

	Оператор	**Оператор с отчетами**	**Ограниченный администратор**	**Администратор**
Сводка	Немедленный запуск резервного копирования и восстановления	Оператор плюс отчеты	Оператор плюс отчеты и планирование операций для указанных доменов политики	Все роли, включая начальное конфигурирование
Класс полномочий ID администратора IBM Spectrum Protect	Нет	Один из следующих классов полномочий: • Хранение • Оператор • Аналитик	Политика (ограниченная) или один из следующих классов полномочий: • Хранение • Оператор • Аналитик	Политика (неограниченная) или Система
Вкладка Резервная копия				

Таблица 11. Доступные функции, основанные на требованиях к полномочиям для ID администратора IBM Spectrum Protect (продолжение)

	Оператор	**Оператор с отчетами**	**Ограниченный администратор**	**Администратор**
Управление задачами резервного копирования **Запустить сейчас**	Да	Да	Да	Да
Управление задачами резервного копирования **Запланировано**	Нет[1]	Нет[1]	Да, в пределах доменов политики	Да
Просмотр задач резервного копирования **Запустить сейчас**	Да	Да	Да	Да
Просмотр задач резервного копирования **Запланировано**	Нет	Да	Да	Да
Удаление задачи резервного копирования **Запланировано**	Нет	Нет	Да, в пределах доменов политики	Да
Вкладка Восстановление				
Запустить задачу **Восстановить**	Да	Да	Да	Да
Вкладка Отчеты				
События	Нет	Да	Да	Да
Последние задачи	Да	Да	Да	Да
Состояние резервного копирования	Нет	Да	Да	Да
Защита приложений	Нет	Да	Да	Да
Занятое пространство центра данных	Нет	Да	Да	Да
Вкладка Конфигурация				
Регистрация узла (Состояние конфигурации -> **Запустить мастер конфигурирования**)	Нет	Нет	Нет[2]	Да

Таблица 11. Доступные функции, основанные на требованиях к полномочиям для ID администратора IBM Spectrum Protect (продолжение)

	Оператор	**Оператор с отчетами**	**Ограниченный администратор**	**Администратор**
Изменение идентификац. данных ID администратора IBM Spectrum Protect (Состояние конфигурации -> **Изменить конфигурацию**)	Да	Да	Да	Да
Изменение пароля узла VMCLI (Состояние конфигурации -> **Изменить конфигурацию**)	Нет	Нет	Да	Да
Изменение доменов графического интерфейса (Состояние конфигурации -> **Изменить конфигурацию**)	Да[3]	Да[3]	Да[3]	Да
Изменение узлов перемещения данных (Состояние конфигурации -> **Изменить конфигурацию**)	Нет	Нет	Нет[2]	Да
Изменить прокси-узлы монтирования (Состояние конфигурации -> **Изменить конфигурацию**)	Нет	Нет	Нет[2]	Да

1. Нельзя зарегистрировать узел, так как требуется неограниченная политика доменов.
2. Вы можете добавить или удалить центры данных VMware и зарегистрировать узлы центра данных.

Чтобы просмотреть уровень полномочий ID администратора IBM Spectrum Protect и соответствующую роль модуля Графический интерфейс Data Protection for VMware vSphere:

1. Перейдите в окно Конфигурация.
2. Щелкните по **Изменить конфигурацию**.
3. Соответствующая информация появится на странице Идентификационные данные сервера Spectrum Protect.

Важное замечание:

- Если уровень полномочий ID администратора IBM Spectrum Protect изменяется на сервере IBM Spectrum Protect, то нужно перезапустить модуль Графический интерфейс Data Protection for VMware vSphere,чтобы изменения вступили в силу.
- Если изменяется роль пользователя, то щелкните по **OK**, чтобы сохранить изменения перед переходом на другую страницу Параметры конфигурации или перед внесением других изменений конфигурации. В ином случае изменения роли пользователя будут утеряны.

Ключи регистрации графического интерфейса Data Protection for VMware

В зависимости от того, какие опции вы выберете при установке, вы можете получить доступ к графическому интерфейсу Data Protection for VMware, используя различные методы. Ключи регистрации создаются для графических интерфейсов Data Protection for VMware.

Фраза “графический интерфейс Data Protection for VMware” применима к следующим графическим интерфейсам:

- Графический интерфейс Data Protection for VMware vSphere, доступ к которому осуществляется в веб-браузере
- IBM Spectrum Protect vSphere Client - Модуль plugin в графическом интерфейсе веб-клиента vSphere

Ключ регистрации компонента IBM Spectrum Protect vSphere Client - Модуль plugin - `com.ibm.tsm.tdpvmware.IBMDataProtection`. Это ключ регистрируется, когда вы выбираете переключатель **Зарегистрировать расширение веб-клиента vSphere** во время установки. На один сервер vCenter регистрируется один экземпляр компонента IBM Spectrum Protect vSphere Client - Модуль plugin.

Ключ регистрации не создается для компонента Графический интерфейс Data Protection for VMware vSphere, доступ к которому вы получаете из веб-браузера.

Чтобы увидеть ключи регистрации, войдите в систему VMware Managed Object Browser (MOB). После входа в систему MOB выберите **Содержимое→Менеджер расширений**, чтобы увидеть ключи регистрации.

Конфигурирование графического интерфейса агент восстановления

В этом разделе содержатся инструкции по конфигурированию графического интерфейса агент восстановления для монтирования, восстановления файлов или быстрого восстановления.

Прежде чем начать

Описанное ниже конфигурирование нужно выполнить до начала работы с графическим интерфейсом агент восстановления.

Важное замечание: Информация о том, как выполнить задачи с использованием графического интерфейса агент восстановления, представлена в электронной справке, устанавливаемой вместе с графическим интерфейсом. Щелкните по **Справка** в любом из окон графического интерфейса, чтобы открыть электронную справку и получить помощь по задачам.

Процедура

1. Зарегистрируйтесь в системе, где вы хотите восстанавливать файлы. На компьютере должен быть установлен агент восстановления.
2. Щелкните по **Выбрать сервер TSM** в графическим интерфейсе агент восстановления, чтобы соединиться с сервером IBM Spectrum Protect. Если агент восстановления установлен на том же компьютере, что Графический интерфейс Data Protection for VMware vSphere и приложения успешно сконфигурированы при помощи мастера конфигурирования интерфейса Графический интерфейс Data Protection for VMware vSphere, то ситуация выглядит так:
   - узел перемещения данных и сервер IBM Spectrum Protect внесены в поле агент восстановления Сервер TSM.
   - В панели Информация о сервере TSM заполнены следующие поля:
     – **Узел аутентификации** содержит список доступных узлов перемещения данных.
     – **Узел назначения** содержит список узлов центра данных, доступных для выбранного узла перемещения данных.

   Если в мастере конфигурирования задан только один локальный узел перемещения данных, то агент восстановления использует этот узел для аутентификации при запуске.агент восстановления запоминает имя последнего узла, подключенного к серверу IBM Spectrum Protect. Если для этого узла (последний подключенный узел) выбрано **Использовать генерирование пароля доступа**, то агент восстановления использует эти идентификационные данные для соединения с сервером IBM Spectrum Protect при запуске. Если соединение с сервером IBM Spectrum Protect ранее не устанавливалось и при помощи мастера сконфигурирован только один узел перемещения данных и только один узел центра данных, то агент восстановления использует эти идентификационные данные для соединения с сервером IBM Spectrum Protect при запуске.

   Задайте следующие параметры:

   Адрес сервера
   Введите IP-адрес или имя хоста IBM Spectrum Protect.

   Порт сервера
   Введите номер порта, используемого для связи с сервером по протоколу TCP/IP. Номер порта по умолчанию - 1500.

   Способ доступа к узлу:

   Asnodename
   Выберите эту опцию, чтобы использовать прокси-узел для доступа к резервным копиям виртуальных машин на узле назначения. Прокси-узел - это узел, которому предоставлены полномочия "прокси" для выполнения операций от имени узла назначения.

   Обычно администратор IBM Spectrum Protect использует для создания взаимосвязи прокси между двумя узлами команду `grant proxynode`.

   Если вы выбрали эту опцию, то сделайте следующее:

   a. Введите имя узла назначения (узел, в котором находятся резервные копии виртуальной машины) в поле **Узел назначения**.
   b. Введите имя прокси-узла в поле **Узел аутентификации**.
   c. Введите пароль для прокси-узла в поле **Пароль**.
   d. Щелкните по **ОК**, чтобы сохранить эти параметры и закрыть информационный диалог IBM Spectrum Protect.

   При использовании этого метода пользователь агент восстановления знает пароль только прокси-узла, и пароль узла назначения защищен.

Fromnode

Выберите эту опцию, чтобы использовать узел с доступом, ограниченным только данными снимков конкретных виртуальных машин на узле назначения.

Обычно этому узлу предоставляется доступ от узла назначения, который владеет резервными копиями виртуальных машин, при помощи команды `set access`:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

Например, эта команда предоставляет узлу `myMountNode` полномочия для восстановления файлов из виртуальной машины `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

Если вы выбрали эту опцию, то сделайте следующее:

a. Введите имя узла назначения (узел, в котором находятся резервные копии виртуальной машины) в поле **Узел назначения**.
b. Введите имя узла, которому предоставляется ограниченный доступ, в поле **Узел аутентификации**.
c. Введите пароль узла, которому предоставляется ограниченный доступ, в поле **Пароль**.
d. Щелкните по **ОК**, чтобы сохранить эти параметры и закрыть информационный диалог IBM Spectrum Protect.

При использовании этого метода вы можете видеть полный список виртуальных машин, для которых созданы резервные копии. Однако можно восстановить только резервные копии виртуальных машин, к которым узлу предоставлен доступ. Кроме того, данные снимков не защищены на сервере от истечения срока годности. Поэтому в этом методе быстрое восстановление не поддерживается

Напрямую

Выберите эту опцию, чтобы аутентификация выполнялась непосредственно на узле назначения (узел, в котором находятся резервные копии виртуальной машины).

Если вы выбрали эту опцию, то сделайте следующее:

a. Введите имя узла назначения (узел, в котором находятся резервные копии виртуальной машины) в поле **Узел аутентификации**.
b. Введите пароль для узла назначения в поле **Пароль**.
c. Щелкните по **ОК**, чтобы сохранить эти параметры и закрыть информационный диалог IBM Spectrum Protect.

Использовать генерирование пароля доступа

Если выбрана эта опция, а поле пароля пустое, то агент восстановления аутентифицируется с существующим паролем, который хранится в реестре. Если опция не выбрана, то нужно ввести пароль вручную.

Чтобы использовать эту опцию, нужно вначале вручную задать начальный пароль для узла, к которому применяется опция. Чтобы задать начальный пароль при первом соединении с узлом IBM Spectrum Protect, нужно ввести пароль в поле **Пароль** и выбрать переключатель **Использовать генерирование пароля доступа**.

Однако если вы используете в качестве **узла аутентификации** локальный узел перемещения данных, то пароль уже может храниться в реестре. Поэтому выберите переключатель **Использовать генерирование пароля доступа** и не вводите пароль.

агент восстановления запросит с заданного сервера список защищенных виртуальных машин и покажет этот список.

3. Щелкните по **Параметры**, чтобы задать следующие опции монтирования, резервного копирования и восстановления:

Кэш записи виртуального тома

Компонент агент восстановления, работающий на хосте прокси резервного копирования Windows, сохраняет изменения данных, созданные при мгновенном восстановлении и монтировании. Эти изменения сохраняются на виртуальном томе в кэше записи. По умолчанию кэш записи разрешен и находится в каталоге `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\`; максимальный размер кэша составляет 90% от объема доступного пространства для выбранной папки. Чтобы системный том не заполнялся, задайте для кэша записи каталог не на системном томе.

Папка для временных файлов

Укажите каталог для сохранения изменений данных. Кэш записи должен находиться на локальном диске; для него нельзя задать каталог в совместно используемой папке. Если кэш записи отключен или переполнен, попытка запустить сеанс быстрого восстановления или монтирования завершится неудачно.

Размер кэша

Задайте максимальный размер кэша записи. Максимальный размер кэша составляет 90% от объема доступного пространства для выбранной папки.

Ограничение: Во избежание прерываний во время обработки восстановления исключите каталог кэша записи из всех параметров защиты антивирусной программы.

Доступ к данным

Укажите тип данных, доступ к которым нужно получить. Если вы используете автономное устройство (например, ленточное устройство или виртуальную ленточную библиотеку), вы должны указать применимый тип данных.

Тип хранения

Укажите одно из следующих устройств хранения, с которого следует монтировать снимок:

Диск/Файл

Снимок монтируется с диска или из файла. Это устройство по умолчанию.

Лента Снимок монтируется из ленточного пула хранения. Если выбрана эту опцию, то смонтировать несколько снимков или запустить операцию быстрого восстановления невозможно.

VTL Снимок монтируется из автономной виртуальной ленточной библиотеки. Поддерживаются параллельные сеансы монтирования в одной и той же виртуальной ленточной библиотеке.

Примечание: При изменении типа хранения нужно перезапустить службу, чтобы изменения вступили в силу.

Запретить защиту от устаревания

Во время выполнения операции монтирования снимок на сервере IBM Spectrum Protect блокируется, чтобы защитить его от устаревания во время выполнения операции. Устаревание может возникнуть, если в смонтированную последовательность снимков добавлен другой снимок. Это значение задает, нужно ли запретить защиту от устаревания во время монтирования.

- Чтобы защитить снимок от устаревания, не выбирайте эту опцию. Снимок на сервере IBM Spectrum Protect заблокирован и защищен от устаревания во время выполнения монтирования.
- Чтобы запретить защиту от устаревания, выберите эту опцию. Эта опция выбрана по умолчанию. Снимок на сервере IBM Spectrum Protect не заблокирован и не защищен от устаревания во время выполнения монтирования. В результате снимок может устареть во время монтирования. Это устаревание может привести к неожиданным результатам и отрицательно повлиять на точку монтирования. Например, точка монтирования может стать непригодной для использования или содержать ошибки. Однако устаревание не влияет на текущую активную копию. Активная копия не может устареть во время операции.

  Если снимок находится на сервере репликации назначения, то заблокировать его нельзя, так как он находится в -режиме 'только для чтения'. Попытка блокировки сервером приведет к ошибке монтирования. Чтобы блокировка не выполнялась и эта ошибка не возникала, выберите эту опцию, чтобы запретить защиту от устаревания.

Размер упреждающего чтения (в блоках по 16 КБ)

Укажите число дополнительных блоков данных, получаемых с устройства хранения после отправки требования чтения одного блока. Значения по умолчанию:

- Диск или файл: 64
- Лента: 1024
- VTL: 64

Максимальное значение для любого устройства равно 1024.

Размер кэша упреждающего чтения (в блоках)

Укажите размер кэша, где будут сохраняться дополнительные блоки данных. Значения по умолчанию:

- Диск или файл: 10000
- Лента: 75000
- VTL: 10000

У каждого снимка есть собственный кэш, поэтому решите, сколько снимков будет монтироваться или восстанавливаться одновременно. Общий размер кэша не может быть больше 75000 блоков.

Тайм-аут драйвера (секунды)

Это значение задает время обработки требований данных от драйвера файловой системы. Если обработка не завершится вовремя, то требование отменяется и драйверу файловой системы возвращается ошибка. При возникновении тайм-аутов можно увеличить это значение. Например, тайм-ауты могут возникать в

медленной сети, при занятости устройства хранения или при обработке нескольких сеансов монтирования или быстрого восстановления. Значения по умолчанию:

- Диск или файл: 60
- Лента: 180
- VTL: 60

Нажмите **OK**, чтобы сохранить изменения и закрыть окно **Параметры**.

4. Убедитесь, что каждый узел сервера IBM Spectrum Protect, указанный опциями `Asnodename` и `Fromnode`, разрешает удаление резервных копий. агент восстановления создает во время работы неиспользуемые временные объекты. Опция сервера `BACKDELete=Yes` дает возможность удалить эти объекты, чтобы они не накапливались в узле.
   a. Войдите на сервер IBM Spectrum Protect и запустите сеанс клиента администрирования в режиме командной строки:
      ```
      dsmadmc -id=admin -password=admin -dataonly=yes
      ```
   b. Введите следующую команду:
      ```
      Query Node <имя_узла> Format=Detailed
      ```
      Убедитесь, что в выходных результатах команды для каждого узла есть следующий оператор:
      ```
      Удаление резервных копий разрешено?: Да
      ```
      Если этого оператора нет, то измените каждый узел следующей командой:
      ```
      UPDate Node <имя_узла> BACKDELete=Yes
      ```
      Еще раз введите команду `Query Node` для каждого узла, чтобы убедиться, что каждый узел разрешает удаление резервных копий.
5. Если вы используете агент восстановления в сети iSCSI и агент восстановления не использует средство перемещения данных, перейдите к файл `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` и задайте тег `[IMOUNT]` и параметр **`Target IP`**:
   ```
   [IMOUNT config]
   Target IP=<IP-адрес сетевой карты на компьютере,
   на котором находятся назначения iSCSI.>
   ```
   Например:
   ```
   [General config]
   param1
   param2
   ...
   [IMount config]
   Target IP=9.11.153.39
   ```
   После добавления или изменения параметра Target IP перезапустите графический интерфейс или интерфейс командной строки Recovery Agent.

Как включить защищенную связь компонента агент восстановления с сервером IBM Spectrum Protect

Если сервер IBM Spectrum Protect сконфигурирован для использования протокола Secure Sockets Layer (SSL) или Transport Layer Security (TLS), вы сможете включить для компонента агент восстановления взаимодействие с сервером с использованием этого протокола.

Прежде чем начать

Прежде чем приступать к конфигурированию защищенных взаимодействий с сервером, рассмотрите следующие требования:

- У каждого сервера, включенного для SSL, должен быть уникальный сертификат. Сертификат может относиться к одному из следующих типов:
  - Самоподписанный сертификат сервера.
  - Сертификат, сгенерированный сертификатом стороннего центра сертификации (certificate authority, CA). Сертификат CA должен быть получен в такой компании, как Symantec или Thawte, или это должен быть внутренний сертификат, хранящийся в вашей компании.
- По соображениям производительности используйте SSL или TLS только для сеансов, для которых требуется защита. Рассмотрите возможность добавления дополнительных процессорных ресурсов в систему сервера, чтобы удовлетворить возросшие требования.
- Чтобы клиент соединялся с сервером, использующим TLS версии 1.2, алгоритмом сигнатуры сертификата должен быть 1 Secure Hash Algorithm 1 (SHA-1) или новее. Если вы используете самоподписанный сертификат для сервера, использующего TSL V1.2, нужно использовать сертификат `cert256.arm`. Вашему администратору IBM Spectrum Protect может потребоваться изменить сертификат по умолчанию на сервере.
- Чтобы выключить протоколы защиты, которые не обеспечивают такую безопасность, как TLS 1.2, добавьте опцию **`SSLDISABLELEGACYtls yes`** в файл `C:\windows\system32\fb.opt` или `C:\Windows\SysWOW64\fb.opt`. TLS 1.2 или новее поможет предотвратить атаки вредоносных программ.

Как включить защищенную связь с использованием самоподписанного сертификата сервера IBM Spectrum Protect

Если сервер IBM Spectrum Protect использует самоподписанный сертификат, вы должны получить копию этого сертификата у администратора сервера и сконфигурировать компонент агент восстановления для взаимодействий с сервером с использованием протокола TLS или SSL.

Об этой задаче

Каждый сервер генерирует свой собственный сертификат. Серверы версии 6.3 и новее генерируют файлы с именем `cert256.arm`, если сервер использует TLS 1.2 или новее, либо `cert.arm`, если сервер использует более раннюю версию SSL или TLS. Версии сервера, более ранние, чем версия 6.3, генерируют файлы с именем `cert.arm` независимо от протокола. Вы должны выбрать сертификат, заданный на сервере как сертификат по умолчанию.

Файл сертификата хранится на рабочей станции сервера в каталоге экземпляра сервера. Например, `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. Если файл сертификата существует, файл сертификата создается при перезапуске сервера с этим набором опций.

Процедура

Чтобы включить взаимодействия SSL или TLS между агентом восстановления и сервером с использованием самоподписанного сертификата:

1. Присоедините путь двоичного файла GSKit и путь библиотеки к переменной среды PATH на клиенте. Например:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Если вы впервые конфигурируете SSL или TLS на клиенте, нужно создать локальную базу данных ключей клиента, dsmcert.kdb. Из каталога `C:\Windows\SysWOW64` запустите команду **gsk8capicmd_64**, как показано в следующем примере:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   Введенный вами пароль используется для шифрования базы данных ключей. Пароль автоматически сохраняется в зашифрованном виде в файле накопления (dsmcert.sth). Файл накопления используется клиентом для получения пароля базы данных ключей.

3. Получите самоподписанный сертификат сервера.

4. Импортируйте сертификат в базу данных dsmcert.kdb. Надо импортировать сертификат для каждого клиента в dsmcert.kdb. Из каталога `C:\Windows\SysWOW64` запустите команду **gsk8capicmd_64**, как показано в следующем примере:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Самоподписанный ключ сервера имя_сервера"
   -file путь_сертификата -format ascii -trust enable
   ```

   В базу данных dsmcert.kdb можно добавить несколько сертификатов сервера, чтобы клиент мог соединяться с разными серверами. Разные сертификаты должны иметь разные метки. Используйте в качестве меток понятные имена.

   Важное замечание: Для аварийного восстановления сервера, если сертификат был потерян, сервер автоматически сгенерирует новый сертификат. Каждый клиент должен затем импортировать новый сертификат.

5. После добавления сертификата в базу данных dsmcert.kdb добавьте опцию `ssl yes` в файл `C:\Windows\SysWOW64\fb.opt` и обновите значение опции `tcpport`.

   Важное замечание:

   Обычно сервер настраивается для соединений SSL или TLS на другом порту, отличном от соединений не SSL и не TLS. Не задавайте номер порта не SSL или не TLS в качестве значения `tcpport`. Если значение `tcpport` - неправильное, агент восстановления не сможет соединиться с сервером.

   Вы не сможете соединиться с портом не SSL или не TLS, используя агент восстановления, включенный для SSL или TLS, и не сможете соединить порт SSL или TLS с агентом восстановления, не включенным для SSL или TLS.

6. Задайте правильные порты SSL или TLS в следующих файлах конфигурации агента восстановления:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Как включить защищенную связь с использованием стороннего сертификата

Если сервер IBM Spectrum Protect использует сертификат, сгенерированный сторонним центром сертификации (certificate authority, CA), вы должны получить корневой сертификат CA.

Об этой задаче

Если сертификат был выдан таким CA, как Symantec или Thawte, клиент готов к SSL или TLS и вы можете пропустить следующие шаги по конфигурированию. Чтобы получить список преинсталлированных корневых сертификатов CA, ищите термин **Корневые сертификаты центров сертификации** в центре знаний IBM.

Если сертификат не сгенерирован преинсталлированным корневым сертификатом или является внутренним сертификатом CA, хранящимся в вашей компании, вы должны сконфигурировать компонент агент восстановления для взаимодействия с сервером, используя протокол TLS или SSL.

Процедура

Чтобы включить взаимодействия SSL или TLS между агентом восстановления и сервером с использованием сертификата CA:

1. Присоедините путь двоичного файла GSKit и путь библиотеки к переменной среды PATH. Например:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Если вы впервые конфигурируете SSL или TLS на клиенте, нужно создать локальную базу данных ключей клиента, dsmcert.kdb. Для клиентов запустите команду **gsk8capicmd_64** из каталога `C:\Windows\SysWOW64` как показано в следующем примере:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw пароль -stash
   ```

   Введенный вами пароль используется для шифрования базы данных ключей. Пароль автоматически сохраняется в зашифрованном виде в файле накопления (dsmcert.sth). Файл накопления используется клиентом для получения пароля базы данных ключей.

3. Получите сертификат CA.

4. Импортируйте сертификат в базу данных dsmcert.kdb. Надо импортировать сертификат для каждого клиента в dsmcert.kdb. Для клиентов запустите команду **gsk8capicmd_64** из каталога `C:\Windows\SysWOW64` как показано в следующем примере:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file путь_корневого_сертификата_CA -format ascii -trust enable
   ```

   В базу данных dsmcert.kdb можно добавить несколько сертификатов сервера, чтобы клиент мог соединяться с разными серверами. Разные сертификаты должны иметь разные метки. Используйте в качестве меток понятные имена.

   Важное замечание: Для аварийного восстановления сервера, если сертификат был потерян, сервер автоматически сгенерирует новый сертификат. Каждый клиент должен импортировать новый сертификат.

5. После добавления сертификата в базу данных dsmcert.kdb добавьте опцию `ssl yes` в файл `C:\Windows\SysWOW64\fb.opt` и обновите значение опции `tcpport`.

   Важное замечание:

Обычно сервер настраивается для соединений SSL или TLS на другом порту, отличном от соединений не SSL и не TLS. Не задавайте номер порта не SSL или не TLS в качестве значения `tcpport`. Если значение `tcpport` - неправильное, агент восстановления не сможет соединиться с сервером.

Вы не сможете соединиться с портом не SSL или не TLS, используя агент восстановления, включенный для SSL или TLS, и не сможете соединить порт SSL или TLS с агентом восстановления, не включенным для SSL или TLS.

6. Задайте правильные порты SSL или TLS в следующих файлах конфигурации агента восстановления:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Параметры локали

Параметры локали указывают язык, используемый для интерфейсов, сообщений и электронной справки.

Графические интерфейсы Data Protection for VMware

Фраза “графический интерфейс Data Protection for VMware” применима к следующим графическим интерфейсам:

- Графический интерфейс Data Protection for VMware vSphere, доступ к которому осуществляется в веб-браузере
- IBM Spectrum Protect vSphere Client - Модуль plugin в графическом интерфейсе веб-клиента vSphere

Графические интерфейсы компонента Data Protection for VMware не поддерживают работу в среде с противоречивыми параметрами локали для разных процессорв, на которых работает графический интерфейс компонента Data Protection for VMware, клиент VMware vSphere Client и сервер IBM Spectrum Protect.

Задайте одни и те же параметры локали на системах, в которых работает графический интерфейс компонента Data Protection for VMware, клиент VMware vSphere и сервер IBM Spectrum Protect.

При первом доступе к странице справки по графическому интерфейсу компонента Data Protection for VMware через ссылку "Узнать подробнее" справка появится на языке, заданном параметром локали системы, в которой работает графический интерфейс компонента Data Protection for VMware. При первом доступе к справке справка не появится на языке, заданном локалью клиента VMware vSphere. В этом случае щелкните после открытия страницы справки графического интерфейса Data Protection for VMware, по крайней мере, по двум ссылкам в справке и закройте справку. В следующий раз, при запуске справки при помощи ссылки "Узнать подробнее" она появится на языке, заданном параметром локали клиента VMware vSphere.

Интерфейс восстановления файлов IBM Spectrum Protect

Содержимое интерфейса и язык приглашений сообщений определяется параметром языка веб-браузера, осуществляющего доступ к интерфейсу восстановления файлов IBM Spectrum Protect.

Для сообщений об ошибках, записываемых в файл `fr_api.log`, интерфейс восстановления файлов IBM Spectrum Protect использует язык, заданный параметром локали системы, в которой работает компонент Графический интерфейс Data Protection for VMware vSphere.

Операции файла журнала

Data Protection for VMware создает и модифицирует несколько файлов журналов во время выполнения операций по установке, резервному копированию, монтированию и восстановлению.

Файлы журнала Data Protection for VMware - это простые текстовые файлы с расширением `.sf`.

Windows Журналы помещаются в следующий каталог:
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`
Каталоги содержат подкаталоги для каждого компонента Data Protection for VMware. Например, подкаталог агент восстановления - это `\mount`, а подкаталог интерфейса командной строки агента восстановления - это `\shell`.
Файлы журналов можн оискать в меню **Windows > Пуск**, выбрав **Панель управления > Поиск** и введя `*.log`.

Linux Журналы помещаются в оба указанных ниже пути:
`<user.home>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
Найти файлы журнала можно при помощи следующей команды:

```
find /opt/tivoli/ -name "*.log"
```

Важное замечание: Существующие файлы журнала перезаписываются при каждом запуске установки. Если вы столкнетесь с проблемой приустановке и вам потребуется переустановить продукт, прежде чем снова приступать к установке, получите существующий файл `TDPVMwareInstallation.log` из каталога `%allusersprofile%`.

Примечание: Когда работает служба Data Protection for VMware, несколько файлов журналов находятся в открытом состоянии. В результате некоторые менеджеры файлов не показывают текущее состояние этих файлов и могут сообщить о нулевом размере файла. Если выбрать или открыть один из этих файлов, менеджеру файлов принудительно обновит сведения о файле.

Файлы журналов агент восстановления

Файл журнала агент восстановления - это `TDP_FOR_VMWARE_MOUNT`*`nnn`*`.sf`. Файл журнала с последними данными - это файл с номером *040* (`TDP_FOR_VMWARE_MOUNT040.sf`). Когда размер журнала достигает максимума, создается новый файл журнала. Имя файла журнала остается тем же, но его номер уменьшается на единицу. Например, данные в файле журнала с номером *040* копируются в файл журнала с номером *039*. Файл журнала с номером *040* содержит самые свежие данные журнала. Когда *040* снова достигает максимального размера, содержимое файла *039* перемещается в файл *038*, а информация из *040* снова перемещается в *039*.

Файлы журнала графического интерфейса Data Protection for VMware

Графический интерфейс Data Protection for VMware vSphere помещает файлы журнала в следующий каталог:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

При файлов журнала убедитесь, что вы включили в сжатый файл все подкаталоги.

Файлы журналов интерфейс командной строки Data Protection for VMware

интерфейс командной строки Data Protection for VMware помещает файлы журналов в следующий каталог:

Windows `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/logs`

При файлов журнала убедитесь, что вы включили в сжатый файл все подкаталоги.

Файлы журнала интерфейса восстановления файлов IBM Spectrum Protect

Интерфейс восстановления файлов IBM Spectrum Protect записывает сообщения в файлы `fr_api.log`, `fr_gui.log` и `messages.log`. Эти файлы находятся в следующем каталоге по умолчанию:

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Имя и расположение файла `fr_api.log` можно изменить, задав опции `API_LOG_FILE_NAME` и `API_LOG_FILE_LOCATION` в файле операций журнала восстановления файлов (`FRLog.config`).

Операции восстановления файлов также записываются сервером IBM Spectrum Protect. Эти сообщения можно искать с помощью административного клиента командной строки сервера.

- Для запуска сеанса клиента администрирования в режиме командной строки введите со своей рабочей станции следующую команду:

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  Если ввести команду **DSMADMC** с опциями **-ID** и **-PASSWORD**, как здесь показано, вас не попросят ввести ID пользователя и пароль.

- Чтобы произвести поиск в суммарной расширенной таблице SQL и увидеть результаты операций восстановления файлов, введите команду **select** на административном клиенте командной строки:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  Поиск можно сузить, включив в оператор выбора один или несколько из следующих критериев:

  - `* ENTITY='`*`ИМЯ_УЗЛА_ПЕРЕМЕЩЕНИЯ_ДАННЫХ`*`'`
  - `* AS_ENTITY='`*`ИМЯ_УЗЛА_ЦЕНТРА_ДАННЫХ`*`'`
  - `* SUB_ENTITY='`*`ИМЯ_ХОСТА_VM`*`'`
  - `* START_TIME='`*`гггг-ММ-дд ЧЧ:мм:сс`*`'`

Например:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
and START_TIME>'2017-03-11 17:30:00'
```

Критерий START_TIME поддерживает запросы со следующими знаками: равно (=), меньше, чем (<), или больше, чем (>).

- Чтобы произвести поиск в таблице журнала операций SQL и увидеть события операций восстановления файлов, введите команду **select** на административном клиенте командной строки:

  ```
  select * from ACTLOG
  ```

  Поиск можно сузить, включив в оператор выбора один или несколько из следующих критериев:

  — * NODENAME='*ИМЯ_УЗЛА_ЦЕНТРА_ДАННЫХ*'

  — * DATE_TIME='*гггг-ММ-дд ЧЧ:мм:сс*'

  Например:

  ```
  select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
  ```

Задавайте значения *ИМЯ_УЗЛА_ПЕРЕМЕЩЕНИЯ_ДАННЫХ* и *ИМЯ_УЗЛА_ЦЕНТРА_ДАННЫХ*, используя символы верхнего регистра.

Критерий ДАТА_ВРЕМЯ поддерживает запросы со следующими знаками: равно (=), меньше, чем (<), или больше, чем (>).

Запуск программы и служб для Data Protection for VMware

По умолчанию, при запуске операционной системы Windows компонент агент восстановления запускается от имени локальной системной учетной записи.

Запуск служб компонента агент восстановления в Microsoft Windows

Пори запуске компонента агент восстановления из меню Пуск в Windows служба автоматически останавливается. Когда агент восстановления, запущенный из меню Пуск, завершает работу, служба автоматически запускается. Кроме того, для этих операционных систем, служба не предоставляет графический интерфейс. Чтобы использовать графический интерфейс, перейдите в меню Пуск в Windows и выберите **Все программы > IBM Spectrum Protect > Data Protection for VMware > агент восстановления**.

интерфейс командной строки Data Protection for VMware

Вы можете проверить, работает ли компонент интерфейс командной строки Data Protection for VMware, выполнив следующую задачу:

Windows Выберите **Пуск > Панель управления > Администрирование > Службы** и убедитесь, что состоянием компонента интерфейс командной строки Data Protection for VMware является Запущен.

Linux Перейдите в каталог scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/) и введите следующую команду:

```
./vmclid status
```

- Если демон не работает, то введите следующую команду, чтобы запустить демон вручную:

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  Для остановки и запуска демона можно также использовать сценарии init:

  ```
  ./vmclid stop
  ./vmclid start
  ```

Приложение A. Расширенное конфигурирование

Нужно вручную сконфигурировать и проверить каждый компонент, используя доступные интерфейсы приложений.

Прежде чем начать

Перед выполнением этой задачи проверьте, выполнено ли следующее:

- Сервер IBM Spectrum Protect должен быть доступен для регистрации узлов.
- Модуль Графический интерфейс Data Protection for VMware vSphere установлен на компьютере, который соответствует требованиям к операционной системе. У него должно быть сетевое соединение со следующими системами:
  - Сервер резервного копирования vStorage
  - Сервер IBM Spectrum Protect
  - Сервер vCenter

Процедура

1. Войдите на сервер IBM Spectrum Protect и выполните действия, описанные в разделе “Настройка узлов IBM Spectrum Protect в среде vSphere” на стр. 96.
2. Войдите на сервер резервного копирования vStorage и выполните действия, описанные в разделе “Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere” на стр. 97.
3. Войдите в систему, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere, и выполните задачи, описанные в разделе “Конфигурирование интерфейс командной строки Data Protection for VMware в среде vSphere” на стр. 103.
4. В системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere, запустите клиент vSphere и войдите в систему vCenter. Если клиент vSphere уже работает, остановите его и перезапустите.
5. Перейдите в каталог Home на клиенте vSphere. Щелкните по значку Графический интерфейс Data Protection for VMware vSphere в панели Решения и приложения.

   Совет: Если значок не показан, это означает. что Графический интерфейс Data Protection for VMware vSphere не зарегистрирован или произошла ошибка соединения.

   a. В меню vSphere Client перейдите в **Модули plugin > Управление модулями plugin**, чтобы запустить менеджер модулей plugin.
   b. Если вы можете найти Графический интерфейс Data Protection for VMware vSphere и произойдет ошибка соединения, проверьте соединение с компьютером, на котором установлен Графический интерфейс Data Protection for VMware vSphere, введя команду `ping`.

Результаты

Графический интерфейс Data Protection for VMware vSphere готов к операциям резервного копирования и восстановления.

Настройка узлов IBM Spectrum Protect в среде vSphere

Эта процедура описывает, как вручную зарегистрировать узлы на сервере IBM Spectrum Protect и предоставить разрешения прокси для этих узлов в среде vSphere.

Прежде чем начать

Важное замечание:

Об этой задаче

Все указанные ниже действия выполняются на сервере IBM Spectrum Protect.

Совет: Эту задачу также можно выполнить, используя мастер конфигурации компонента Графический интерфейс Data Protection for VMware vSphere или блокнот изменения конфигурации. Запустите Графический интерфейс Data Protection for VMware vSphere, открыв веб-браузер и перейдя на веб-сервер графического интерфейса. Например:

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Войдите в систему, указав ID пользователя vCenter и пароль.

- Для начального конфигурирования перейдите в **Конфигурация > Запустить мастер конфигурирования**.
- Для существующей конфигурации перейдите в **Конфигурация > Правка конфигурации**.

Процедура

1. Войдите на сервер IBM Spectrum Protect и запустите сеанс клиента администрирования в режиме командной строки:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Введите команду `REGister Node`, чтобы зарегистрировать на сервере IBM Spectrum Protect следующие узлы:

   a. Узел, соответствующий VMware vCenter (узел vCenter):

      ```
      REGister Node MY_VCNODE <пароль для MY_VCNODE>
      ```

   b. Узел, который взаимодействует с IBM Spectrum Protect и Графический интерфейс Data Protection for VMware vSphere (узел VMCLI):

      ```
      REGister Node MY_VMCLINODE <пароль для MY_VMCLINODE>
      ```

   c. Узел, соответствующий центру данных и являющийся местом, где хранятся данные VM (узел центра данных):

      ```
      REGister Node MY_DCNODE <пароль для MY_DCNODE>
      ```

   d. Узел, перемещающий данные с одного компьютера на другой (узел перемещения данных):

      ```
      REGister Node MY_DMNODE <пароль для MY_DMNODE>
      ```

   Внимание: При регистрации узлов на сервере IBM Spectrum Protect не используйте параметр `userid`.

3. Введите команду `GRant PROXynode`, чтобы задать взаимосвязи прокси для этих узлов:

   Напоминание: Узлы назначения содержат данные, а узлы-агенты выступают от имени узлов назначения. При предоставлении полномочий прокси узлу назначения узел-агент может выполнять операции резервного копирования и восстановления для узла назначения.

a. Предоставьте авторизацию прокси объекту узел vCenter, введя следующую команду:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Эта команда предоставляет MY_DCNODE и MY_VMCLINODE полномочия для резервного копирования и восстановления виртуальных машин от имени MY_VCNODE.

b. Предоставьте авторизацию прокси объекту узел центра данных, введя следующую команду:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Эта команда предоставляет MY_VMCLINODE и MY_DMNODE полномочия для резервного копирования и восстановления виртуальных машин от имени MY_DCNODE.

c. (Необязательно) Предоставьте полномочия прокси всем дополнительным объектам узел центра данных или узлам перемещения данных в вашей среде.

d. Проверьте взаимосвязи прокси: введите на сервере IBM Spectrum Protect команду Query PROXynode. Ниже показаны ожидаемые выходные результаты команды: Ожидаемые выходные результаты команды:

```
Target Node         Agent Node
--------------    ------------------------------
MY_VCNODE           MY_DCNODE  MY_VMCLINODE
MY_DCNODE           MY_VMCLINODE  MY_DMNODE
```

Дальнейшие действия

Следующая операция конфигурирования вручную, выполняемая после успешной настройки узлов IBM Spectrum Protect - настройка узлов перемещения данных (смотрите раздел “Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere”).

Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere

Если вы выгрузите рабочую нагрузку по резервному копированию на сервер резервного копирования vStorage в среде vSphere, вы можете с помощью мастера перемещения данных настроить ряд узлов перемещения данных для выполнения операций и перемещения данных на сервер IBM Spectrum Protect.

Прежде чем начать

Для настройки узлов перемещения данных требуется произвести изменения конфигурации, запустить необходимые службы и проверить настройку.

Эти задачи можно выполнить с помощью графического пользовательского интерфейса модуля plugin, что позволяет упростить и ускорить процесс создания ряда узлов перемещения данных. Либо можно выполнить эти действия вручную; дополнительную информацию смотрите в разделе “Настройка узлов перемещения данных вручную в среде vSphere” на стр. 99.

В стандартной среде Data Protection for VMware для каждого компонента узел перемещения данных используется отдельный файл dsm.opt (Windows) или раздел файла dsm.sys (Linux). Если несколько узлов перемещения данных на сервере резервного копирования vStorage используются для дедупликации данных и у этих

узлов есть разрешения на перемещение данных для одного и того же объекта узел центра данных, каждый файл `dsm.opt` или раздел файла `dsm.sys` должен содержать свое значение опции `dedupcachepath`.

Узел перемещения физических данных обычно использует SAN для резервного копирования и восстановления данных. Если вы конфигурируете узел перемещения данных для непосредственного доступа к томам хранения, то отключите автоматическое назначение букв дисков. Если вы не отключите назначение букв дисков, то клиент на узле перемещения данных может повредить отображение неструктурированных данных (Raw Data Mapping, RDM) виртуальных дисков. Если RDM виртуальных дисков повреждено, то резервное копирование выполнить невозможно.

Ограничение: Data Protection for VMware не поддерживает расписание сервера резервного копирования vStorage (используется в качестве узла перемещения данных) для резервного копирования самого себя. Убедитесь, что сервер резервного копирования vStorage исключен из своих расписаний. Используйте другой сервер резервного копирования vStorage для резервного копирования виртуальной машины, которая содержит сервер резервного копирования vStorage.

Если вам нужно выполнить какие-либо из указанных выше настроек, смотрите раздел "Как вручную настроить узлы перемещения данных в среде vSphere".

Об этой задаче

Используйте модуль plug-in vSphere, чтобы сконфигурировать узлы перемещения данных.

Процедура

1. В модуле plugin vSphere выберите IBM Spectrum Protect.
2. На вкладке **Конфигурировать** выберите **Средства перемещения данных**.
3. В панели **Добавить средства перемещения данных** выберите в выпадающем меню центр данных.
4. Измените нужным вам образом следующие поля:
   - **Имя средства перемещения данных**: Имя узла, в качестве которого уже подставлено рекомендуемое имя на основе префикса узла, имени узла центра данных, имени средства перемещения данных и увеличивающегося номера.
   - **Имя хоста функции перемещения данных**
   - **Пользователь vCenter**, в качестве которого уже подставлено имя пользователя, зарегистрировавшего модуль plug-in.
   - **Пароль vCenter**

   Щелкните по **Добавить**, когда закончите работу с параметрами.
5. В окне **Результаты** будет показано следующее:
   - Имя сконфигурированного средства перемещения данных.
   - Расположение файла опций. Внося изменения в этот файл, можно сконфигурировать средство перемещения данных.
   - Расположение файлов журналов.
   - Опции по умолчанию, которые использовались.
6. Теперь вы можете протестировать средство перемещения данных, используя вкладку **IBM Spectrum Protect > Конфигурировать средства перемещения данных**.

Также можно проверить установку, выбрав средство перемещения данных и нажав на **Проверить** либо проверив состояние при следующем добавлении средства перемещения данных.

7. Средство перемещения данных можно добавить в расписание, используя вкладку **IBM Spectrum Protect > Расписания**.

Настройка узлов перемещения данных вручную в среде vSphere

Если вы выгрузите рабочую нагрузку по резервному копированию на сервер резервного копирования vStorage в среде vSphere, вы можете вручную настроить узлы перемещения данных для выполнения операций и перемещения данных на сервер IBM Spectrum Protect.

Прежде чем начать

Узел перемещения физических данных обычно использует SAN для резервного копирования и восстановления данных. Если вы конфигурируете узлы перемещения данных для непосредственного доступа к томам хранения, то отключите автоматическое назначение букв дисков. Если вы не отключите назначение букв дисков, то клиент на узле перемещения данных может повредить отображение неструктурированных данных (Raw Data Mapping, RDM) виртуальных дисков. Если RDM виртуальных дисков повреждено, то резервное копирование выполнить невозможно.

Обязательные службы: Функции перемещения данных требуется служба приемника клиента, служба удаленного агента клиента и служба планировщика клиента, о чем говорится в следующих шагах. Если вы удалите функцию перемещения данных из центра данных, деинсталлируйте и удалите эти службы для функции перемещения данных.

Важное замечание: Если узел перемещения данных не установлен в той же системе Windows, что и компонент Графический интерфейс Data Protection for VMware vSphere, и если при конфигурировании узла перемещения данных была выбрана опция **Создать службы**, описанные ниже шаги не требуются.

В стандартной среде Data Protection for VMware для каждого компонента узел перемещения данных используется отдельный файл `dsm.opt` (Windows) или раздел файла `dsm.sys` (Linux). Если несколько узлов перемещения данных на сервере резервного копирования vStorage используются для дедупликации данных и у этих узлов есть разрешения на перемещение данных для одного и того же объекта узел центра данных, каждый файл `dsm.opt` или раздел файла `dsm.sys` должен содержать свое значение опции `dedupcachepath`. Чтобы добиться наилучших результатов, задайте разные значения опций `schedlogname` и `errorlogname` для каждого файла `dsm.opt` или раздела файла `dsm.sys`. Минимальный набор обязательных опций приведен в описании шага 2.

Узел перемещения физических данных обычно использует SAN для резервного копирования и восстановления данных. Если вы конфигурируете узел перемещения данных для непосредственного доступа к томам хранения, то отключите автоматическое назначение букв дисков. Если вы не отключите назначение букв дисков, то клиент на узле перемещения данных может повредить отображение неструктурированных данных (Raw Data Mapping, RDM) виртуальных дисков. Если RDM виртуальных дисков повреждено, то резервное копирование выполнить невозможно.

Ограничение: Data Protection for VMware не поддерживает расписание сервера резервного копирования vStorage (используется в качестве узла перемещения данных) для резервного копирования самого себя. Убедитесь, что сервер резервного копирования vStorage исключен из своих расписаний. Используйте другой сервер резервного копирования vStorage для резервного копирования виртуальной машины, которая содержит сервер резервного копирования vStorage.

Об этой задаче

Совет: Все указанные ниже действия выполняются на сервере резервного копирования vStorage.

Процедура

1. Linux Убедитесь, что на компьютере назначения установлена программа Java.
2. Linux Задайте соответствующие переменные среды.
   a. Убедитесь, что переменная среды `JAVA_HOME` экспортирована правильно:
      ```
      export JAVA_HOME=<jre-or-jdk-install-dir>
      ```
   b. Убедитесь, что переменная среды `PATH` экспортирована правильно:
      ```
      export PATH=$PATH:$JAVA_HOME/jre/bin
      ```
   c. Убедитесь, что переменная среды `LD_LIBRARY_PATH` экспортирована правильно. Проверьте ее или задайте в качестве ее значения каталог установки клиента и совместно используемую библиотеку Java, `libjvm.so`:

      Для IBM Java :
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
      ```
      Для Oracle Java :
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
      ```
3. Создайте файл опций `dsm.opt` или `dsm.sys` в следующем расположении:
   - **Windows:** `C:\Program Files\Tivoli\TSM\baclient`
   - **Linux:** `/opt/tivoli/tsm/client/ba/bin`
4. Скопируйте опции из примера файла опций для узла перемещения данных в файл `dsm.opt` или `dsm.sys`. Чтобы найти файл примеров для узла перемещения данных:
   - Откройте браузер и введите адрес веб-сервера графического интерфейса: Например:
     ```
     https://guihost.mycompany.com:9081/TsmVMwareUI/
     ```
   - Войдите в систему, указав имя пользователя и пароль и убедившись, что выбран **Режим конфигурирования**.
   - В мастере конфигурирования перейдите на страницу Узлы перемещения данных.
   - Найдите нужный вам узел перемещения данных и щелкните по **Представление**.
   - Скопируйте примеры опций с вкладки **Windows** или **Linux** в файл опций.

   При необходимости вы сможете настроить эти опции для вашей среды.

   Описание опций смотрите в разделе Справочник по опциям.

   Для операций мгновенного доступа, мгновенного восстановления или монтирования (восстановления файлов) обязательно добавьте `VMISCSISERVERADDRESS` в файл опций узла перемещения данных. Задайте IP-адрес сервера iSCSI сетевой карты на сервере резервного копирования vStorage, который используется для передачи данных iSCSI во время быстрых операций. Физическая сетевая карта, привязанная к устройству iSCSI на хосте ESX, должна находиться в той же подсети, что и сетевая карта сервера резервного копирования vStorage, который используется для передачи данных iSCSI.

5. Введите следующую команду, чтобы задать пользователя и пароль vCenter VMware для узла перемещения данных:

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <администратор> <пароль1>
   ```

6. Настройте службу приемника клиента и службу планировщика перемещения данных, выполнив следующие задачи:

   - Windows В этой процедуре используется мастер конфигурирования графического интерфейса клиента IBM Spectrum Protect, чтобы настроить службу приемника клиента и службу планировщика. По умолчанию служба агента удаленного клиента также настраивается с помощью этого мастера. Если вы используете утилиту конфигурирования клиентской службы IBM Spectrum Protect, (**dsmcutil**) для этой задачи, обязательно установите службу агента удаленного клиента.

     Запустите мастер конфигурирования клиента IBM Spectrum Protect из меню Файл: перейдите в **Утилиты > Мастер настройки**:

     – Выберите **Сконфигурировать веб-клиент TSM**. Введите нужные данные.

       a. Для опции Когда вы хотите запустить службу? выберите **Автоматически при загрузке Windows**.

       b. Для опции Запустить службу по завершении работы этого мастера? выберите **Да**.

       Когда операция будет успешно выполнена, вернитесь на начальную страницу мастера и перейдите к шагу b.

       Совет: Если вы конфигурируете на одном компьютере несколько узлов перемещения данных, то для каждого экземпляра акцептора клиента нужно задать свой номер порта.

     – Выберите Сконфигурировать планировщик клиента TSM. Введите нужные данные.

       a. При вводе имени планировщика убедитесь, что выбрана опция **Использовать для управления планировщиком Client Acceptor Daemon (CAD)**.

       b. Для опции Когда вы хотите запустить службу? выберите **Автоматически при загрузке Windows**.

       c. Для опции Запустить службу по завершении работы этого мастера? выберите **Да**.

   - Linux **Для узла перемещения данных в Linux выполните следующие шаги:**

     a. Программа установки создает сценарий запуска Client Acceptor Daemon (dsmcad) в /etc/init.d. Проверьте ее или задайте соответствующие переменные среды в файле /etc/init.d/dsmcad.

     b. Задайте следующие опции в файле dsm.sys, в разделе узел перемещения данных:

        – Задайте опцию managedservices со следующими двумя параметрами:

          ```
          managedservices schedule webclient
          ```

          Эта опция указывает, что демон Client Acceptor управляет и веб-клиентом, и планировщиком.

        – (Необязательно) Если вы хотите направлять информацию о расписании и ошибках в файлы журнала, отличные от файлов по умолчанию, то задайте опции schedlogname и errorlogname с полным именем файла, в котором следует сохранять информацию журнала. Например:

          ```
          schedlogname /vmsched/dsmsched_dm.log
          errorlogname /vmsched/dsmerror_dm.log
          ```

c. Запустите службу приемника клиента.

Client Acceptor Daemon должен быть запущен, чтобы он мог управлять операциями планировщика или веб-клиентом. От имени пользователя root выполните следующие шаги:

1) Сконфигурируйте службу приемника клиента и службу планировщика перемещения данных, так чтобы они работали как сервер резервного копирования vStorage.

2) Запустите приемник клиента, введя следующую команду:

```
service dsmcad start
```

Чтобы приемник клиента запускался автоматически после перезапуска системы, добавьте в окне приглашения оболочки следующую службу:

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

Совет: Если вы хотите запускать команду **dsmc** непосредственно из командной строки Linux, вы также должны применить к командной оболочке эквивалентные переменные среды, о которых говорилось в шаге 2.

7. Запустите сеанс командной строки перемещения данных с использованием параметров командной строки `-asnodename` и `-optfile`:

```
dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
```

Убедитесь, что после начального входа в систему у вас не запрашивают пароль.

Внимание: Во избежание сбоя планировщика IBM Spectrum Protect убедитесь, что опция `asnodename` не задана в файле `dsm.opt` (Windows) или в разделе файла `dsm.sys` (Linux). Планировщик запрашивает на сервере IBM Spectrum Protect расписания, связанные с `nodename` (узел перемещения данных), а не с `asnodename` (узел центра данных). Если в файле `dsm.opt` или `dsm.sys` задана опция `asnodename`, то запрашиваются расписания, связанные с `asnodename`, а не с `nodename`. В результате операции расписания завершаются неудачно.

Сделайте следующее:

a. Проверьте соединение с сервером IBM Spectrum Protect: введите команду

```
dsmc query session
```

Эта команда выводит информацию о сеансе, включая текущее имя узла, время установления сеанса, информацию о сервере и о соединении с сервером.

b. Убедитесь, что вы можете выполнить резервное копирование виртуальной машины: введите команду

```
dsmc backup vm vm1
```

На шагах 5b и 5d `vm1` - это имя виртуальной машины.

c. Убедитесь, что резервное копирование успешно выполнено: введите команду

```
dsmc query vm "*"
```

d. Убедитесь, что виртуальную машину можно восстановить: введите команду

```
dsmc restore vm vm1 -vmname=vm1-restore
```

8. Убедитесь, что акцептор и агент клиента сконфигурированы правильно:

a. Введите в окне веб-браузера адрес IBM Spectrum Protect vSphere Client - Модуль plugin. Например:

```
https://guihost.mycompany.com/vsphere-client/
```

b. Войдите в систему с именем пользователя и паролем vCenter.

c. На веб-клиенте vSphere выберите **IBM Spectrum Protect > Конфигурирование > Средства перемещения данных**.

d. Убедитесь, что в столбце **Состояние** для узла перемещения данных показано значение **Проверено**. Если показано значение **Неудачно**, наведите указатель мыши на состояние, чтобы увидеть сообщение о неудачном выполнении.

Совет: Если IP-адрес изменится в системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere, вы должны будете выполнить следующее:

a. Снова настройте акцептор клиента, чтобы компонент Графический интерфейс Data Protection for VMware vSphere был включен для операций. В противном случае менеджер plug-in покажет состояние Графический интерфейс Data Protection for VMware vSphere как выключенное.

Конфигурирование интерфейс командной строки Data Protection for VMware в среде vSphere

Измените профиль интерфейс командной строки Data Protection for VMware в системе, где установлен Графический интерфейс Data Protection for VMware vSphere.

Прежде чем начать

Профиль (`vmcliprofile`) расположен в следующем каталоге на компьютере, на котором установлен модуль Графический интерфейс Data Protection for VMware vSphere:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64-Разрядная система: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

Об этой задаче

Все указанные ниже действия выполняются в системе, где установлен компонент Графический интерфейс Data Protection for VMware vSphere.

Совет: Эту задачу также можно выполнить, используя мастер конфигурации компонента Графический интерфейс Data Protection for VMware vSphere или блокнот конфигурации. Перейдите в окно Конфигурация компонента Графический интерфейс Data Protection for VMware vSphere и щелкните по **Запустить мастер конфигурирования** или по **Изменить конфигурацию**.

Процедура

1. Задайте в профиле следующие параметры:

   VE_TSMCLI_NODE_NAME
   Задайте узел, соединяющий компонент интерфейс командной строки Data Protection for VMware с сервером IBM Spectrum Protect и агентом узла (`MY_VMCLINODE`).

   Ограничение: узел VMCLI не поддерживает протокол SSL или аутентификацию LDAP при соединении с сервером IBM Spectrum Protect.

   VE_VCENTER_NODE_NAME
   Задайте виртуальный узел, представляющий vCenter (`MY_VCNODE`).

VE_DATACENTER_NAME

Задайте виртуальный узел, отображаемый в центр данных. Синтаксис: `имя_центра_данных::имя_узла_центра_данных`

- В значении `имя_центра_данных` учитывается регистр.
- Убедитесь, что этот параметр задан для каждого центра данных в среде (`MY_DCNODE`).
- Графический интерфейс Data Protection for VMware vSphere не поддерживает центры данных с таким же именем в vCenter.

VE_TSM_SERVER_NAME

Задайте имя хоста или IP-адрес сервера IBM Spectrum Protect.

VE_TSM_SERVER_PORT

Задайте номер порта для сервера IBM Spectrum Protect. Значение по умолчанию - `1500`.

Ниже приведен пример профиля с этими параметрами:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. Задайте пароль для компонента узел VMCLI в файле `pwd.txt`.
Этот пароль предназначен для узла, который соединяет компонент интерфейс командной строки Data Protection for VMware с сервером IBM Spectrum Protect и объектом узел перемещения данных. Задается в параметре профиля VE_TSMCLI_NODE_NAME.
   a. Введите команду `echo`, чтобы создать текстовый файл, содержащий пароль.

      Linux `echo password1 > pwd.txt`

      Windows `echo password1> pwd.txt`

      Windows Между паролем (`password1`) и символом больше, чем (`>`), не должно быть пробела.

   b. Введите эту команду vmcli, чтобы задать пароль для компонента узел VMCLI:
      `vmcli -f set_password -I pwd.txt`

      Важное замечание:

      - Linux Команду `vmcli -f set_password` нужно вводить от имени пользователя tdpvmware, а не от имени пользователя root.
      - Linux Windows Если вы собираетесь генерировать отчеты о защите приложений, вы должны задать параметр **`-type VMGuest`**, чтобы указать, что пароль применяется к VM. Например:

        ```
        vmcli -f set_password -type VMGuest -I password.txt
        ```

3. Убедитесь, что работает интерфейс командной строки Data Protection for VMware:

   Windows Выберите **Пуск > Панель управления > Администрирование > Службы** и убедитесь, что состоянием компонента `интерфейс командной строки Data Protection for VMware` является `Запущен`.

   Linux Перейдите в каталог scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) и введите следующую команду:

   ```
   ./vmclid status
   ```

   - Если демон работает, то переходите к шагу 4.

- Если демон не работает, то введите следующую команду, чтобы запустить демон вручную:

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  Для остановки и запуска демона можно также использовать сценарии init:

  ```
  ./vmclid stop
  ./vmclid start
  ```

4. Введите следующую команду vmcli, чтобы убедиться, что объект интерфейс командной строки Data Protection for VMware распознает конфигурацию узла IBM Spectrum Protect:

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Проверьте узлы, чтобы убедиться, что нет никаких ошибок конфигурации:
   a. Запустите модуль Графический интерфейс Data Protection for VMware vSphere, щелкнув по значку в окне Решения и приложения клиента vSphere.
   b. Перейдите в окно Конфигурация.
   c. Выберите узел в таблице и щелкните по **Проверить выбранные узлы**. В панели Информация о состоянии будет показана информация о состоянии.

Дальнейшие действия

Linux Windows После успешного выполнения операций конфигурирования вручную, описанных в этом разделе:

1. “Настройка узлов IBM Spectrum Protect в среде vSphere” на стр. 96
2. “Настройка узлов перемещения данных с помощью графического пользовательского интерфейса модуля plug-in vSphere” на стр. 97

Для резервного копирования ваших данных VM никаких дополнительных задач по конфигурированию не требуется.

Контрольный список конфигурации интерфейса командной строки среды vSphere

Используйте эту процедуру, чтобы сконфигурировать Data Protection for VMware в среде vSphere, используя только интерфейс командной строки.

Процедура

Выполните шаги 1 и 2 на сервере IBM Spectrum Protect.

1. Зарегистрируйте на сервере IBM Spectrum Protect следующие узлы:
   a. Узел, соответствующий VMware vCenter (узел vCenter):

      ```
      REGister Node MY_VCNODE <пароль для MY_VCNODE>
      ```

   b. Узел, который взаимодействует с IBM Spectrum Protect и Графический интерфейс Data Protection for VMware vSphere (узел VMCLI):

      ```
      REGister Node MY_VMCLINODE <пароль для MY_VMCLINODE>
      ```

   c. Узел, соответствующий центру данных и являющийся местом, где хранятся данные VM (узел центра данных):

      ```
      REGister Node MY_DCNODE <пароль для MY_DCNODE>
      ```

   d. Узел, перемещающий данные с одного компьютера на другой (узел перемещения данных):

      ```
      REGister Node MY_DMNODE <пароль для MY_DMNODE>
      ```

2. Задайте взаимосвязи прокси для следующих узлов:

a. Предоставьте авторизацию прокси объекту узел vCenter, введя следующую команду:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Эта команда предоставляет MY_DCNODE и MY_VMCLINODE полномочия для резервного копирования и восстановления виртуальных машин от имени MY_VCNODE.

b. Предоставьте авторизацию прокси объекту узел центра данных, введя следующую команду:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Эта команда предоставляет MY_VMCLINODE и MY_DMNODE полномочия для резервного копирования и восстановления виртуальных машин от имени MY_DCNODE.

c. (Необязательно) Предоставьте полномочия прокси всем дополнительным объектам узел центра данных или узлам перемещения данных в вашей среде.

d. Проверьте взаимосвязи прокси: введите на сервере IBM Spectrum Protect команду Query PROXynode. Ниже показаны ожидаемые выходные результаты команды:

```
Target Node         Agent Node
--------------    ------------------------------
MY_VCNODE              MY_DCNODE  MY_VMCLINODE
MY_DCNODE            MY_VMCLINODE  MY_DMNODE
```

Выполните на сервере резервного копирования vStorage шаги 3 - 9.

3. Задайте соответствующие значения для следующих опций перемещения данных:

   - Windows Задайте эти опции в файле опций dsm.opt.
   - Linux Задайте эти опции в файле dsm.sys, в разделе узел перемещения данных.

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

Примечание: Опция HTTPPORT требуется, только если используется несколько служб Client Acceptor (CAD). Например, если есть два узла перемещения данных (и две службы CAD), то в файле опций для каждого узла перемещения данных нужно задать свое значение HTTPPORT.
Ниже приведен пример файла dsm.dm.opt с этими опциями:

```
NODename MY_DMNODE
PASSWORDAccess              generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort                     1500
COMMMethod tcpip
HTTPPORT 1583
```

4. Проверьте соединение с сервером IBM Spectrum Protect: введите команду dsmc query session

5. Введите следующую команду, чтобы задать пользователя и пароль vCenter VMware для узла перемещения данных:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <администратор> <пароль1>`
6. Настройте следующие службы IBM Spectrum Protect:
   - Windows
     a. Установите службу Scheduler:
        ```
        dsmcutil install scheduler /name:"TSM Central Scheduler Service"
        /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
        ```
     b. Установите CAD:
        ```
        dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
        ```
     c. Установите службу Remote Client Agent:
        ```
        dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /partnername:"TSM CAD - MY_DMNODE" /startnow:no
        ```
   - Linux Задайте опцию `managedservices` в файле `dsm.sys`, в разделе узел перемещения данных:
     Задайте параметры `schedule` и `webclient`:
     ```
     managedservices schedule webclient
     ```
     Эта опция указывает, что демон Client Acceptor управляет и веб-клиентом, и планировщиком.
7. Linux Чтобы сконфигурировать службу акцептора клиента и службу планировщика перемещения данных, так чтобы они работали как сервер резервного копирования vStorage, задайте в файле `/etc/init.d/dsmcad` следующую переменную среды:
   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```
8. Linux Запустите службу Client Acceptor: Программа установки создает сценарий запуска демона Client Acceptor Daemon (`dsmcad`) в `/etc/init.d`. Демон Client Acceptor Daemon должен быть запущен, чтобы он мог управлять операциями планировщика или веб-клиентом. Введите как пользователь root следующую команду, чтобы запустить демон:
   ```
   service dsmcad start
   ```
   Чтобы демон Client Acceptor Daemon запускался автоматически после перезапуска системы, добавьте в окне приглашения оболочки следующую службу:
   ```
   # chkconfig --add dsmcad
   ```
9. Убедитесь, что службы IBM Spectrum Protect правильно настроены:
   a. Войдите в удаленную систему.
   b. Соединитесь с компьютером `HOST1` при помощи веб-браузера, используя следующие адрес и порт:
      `http://HOST1.xyz.yourcompany.com:1581`

Выполните шаг 10 в системе, в которой установлен компонент Графический интерфейс Data Protection for VMware vSphere.

10. Задайте соответствующие значения для следующих опций в профиле интерфейс командной строки Data Protection for VMware (`vmcliprofile`):

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

Ниже приведен пример профиля с этими опциями:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

Профиль находится в следующих каталогах:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64-Разрядная система: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

a. Задайте пароль для компонента узел VMCLI:

   1) Введите команду `echo`, чтобы создать текстовый файл, содержащий пароль.

      Linux

      ```
      echo password1 >
      pwd.txt
      ```

      Windows

      ```
      echo password1> pwd.txt
      ```

   2) Введите эту команду vmcli, чтобы задать пароль для компонента узел VMCLI:

      Важное замечание: Linux Эту команду нужно вводить от имени пользователя tdpvmware, а не root.

      ```
      vmcli -f set_password -I pwd.txt
      ```

b. Убедитесь, что работает интерфейс командной строки Data Protection for VMware:

   Windows Введите эту команду из командной строки Windows:

   ```
   net start
   ```

   Linux Введите команду:

   ```
   ./vmclid status
   ```

c. Введите следующую команду vmcli, чтобы убедиться, что объект интерфейс командной строки Data Protection for VMware распознает конфигурацию узла IBM Spectrum Protect:

   ```
   vmcli -f inquire_config -t TSM
   ```

Рекомендации по конфигурированию ленточных устройств

Прочтите эти рекомендации, прежде чем пытаться выполнять операции резервного копирования с использованием ленточных устройств хранения.

Подготовка к резервному копированию на ленту

Linux Windows Перед выполнением резервного копирования на ленту на сервере IBM Spectrum Protect для ленточного устройства нужно задать следующие параметры:

1. Задайте класс управления:

   ```
   define mgmtclass <имя_домена> <имя_набора_политик> <имя_класса_управления>
   ```

   Например:

   ```
   define mgmtclass tape tape DISK
   ```

2. Задайте группу копирования:

   ```
   define copygroup <имя_домена> <имя_набора_политик> <имя_класса_управления>
   destination=<имя_пула_stg>
   ```

   Например:

   ```
   define copygroup tape tape DISK destination=Diskpool
   ```

3. Активируйте набор политик:

   ```
   activate policyset <имя_домена> <имя_набора_политик>
   ```

   Например:

   ```
   activate policyset tape tape
   ```

При конфигурировании резервного копирования на физический ленточный носитель существуют дополнительные требования к конфигурации. Всегда сохраняйте метаданные IBM Spectrum Protect (управляющие файлы) на диске, а фактические данные резервных копий виртуальных машин - на ленте.

- Опция VMMC позволяет сохранять резервные копии VMware (и управляющие файлы VMware) с использованием класса управления, отличающегося от класса управления по умолчанию.
- Используйте опцию VMCTLMC, чтобы указать, какой класс управления следует использовать для управляющих файлов VMware при резервном копировании VMware. Указанный вами класс управления переопределит класс управления по умолчанию. Он также переопределит класс управления, заданный опцией VMMC. Класс управления VMCTLMC должен задавать дисковый пул хранения без переноса на ленту.
- Опция VMMC всегда используется для управления хранением резервных копий виртуальной машины. Эта опция применима как к конфигурациям с использованием дисковых устройств, так и к конфигурациям с использованием ленточных устройств. VMCTLMC не используется для управления хранением управляющих файлов. Управляющие файлы и файлы данных входят в одну группу и срок их годности истекает одновременно, в соответствии с политикой хранения, заданной опцией VMMC. Если заданы обе опции, то VMMC используется для файлов данных, а VMCTLMC - для управляющих файлов.

Ограничение: Операции восстановления, использующие агенты хранения в конфигурации без локальной сети, могут восстанавливать файлы из пула хранения копий, даже если данные можно извлечь из основного пула хранения. Это может произойти, если требование восстановления относится к конкретному файлу или если в требовании восстановления не используется метод 'без запроса', а основная копия файла хранится в пуле хранения, который недоступен без локальной сети. Это может также повлиять на ситуации, не связанные с восстановлением (например, на операции резервного копирования Data Protection for VMware). В среде Data Protection for VMware предпочтительный метод хранения файлов управления виртуальной машины - диск, чтобы для восстановления файлов во время инкрементного резервного копирования не требовалось монтирование. Эти файлы управления виртуальной машины не только должны быть помещены на диск; они не должны копироваться в пул хранения копий, который доступен без локальной сети. В таком случае при восстановлении файлов во время инкрементного резервного копирования без локальной сети с клиента Data Protection for VMware будет использоваться монтирование ленты.

Если в среде сервера IBM Spectrum Protect используется перенос с диска на ленту, то перед переносом примите во внимание следующие рекомендации:

- Присвойте параметру MIGDELAY для дискового пула хранения значение, поддерживающее выполнение большинства требований монтирования с диска. При типичном использовании высокий процент восстановления отдельных файлов достигается за несколько дней. Например, обычно проходит 3-5 дней с момента последнего изменения файла. Поэтому рассмотрите возможность хранить данные за этот короткий период на диске, чтобы оптимизировать операции восстановления.

  Кроме того, если для дискового пула хранения используется дедупликация данных на стороне клиента, то задайте для опции MIGDELAY значение с учетом частоты операций полного резервного копирования виртуальной машины. Не переносите данные из дедуплицированного пула хранения на ленту, пока для виртуальной машины не будет выполнено хотя бы две операции полного резервного копирования. После перемещения данных на ленту дедупликация больше не выполняется. Например, если операции полного резервного копирования выполняются еженедельно, рассмотрите возможность задать для параметра MIGDELAY значение, равное, как минимум, 10 дням. Такое значение параметра будет гарантировать, что каждая операция полного резервного копирования выявит и использует дубликаты данных из предыдущей резервной копии до перемещения данных на ленту.
- Используйте пул хранения, относящийся к классу устройств FILE, а не пул хранения, относящийся к классу устройств DISK. Типичное значение размера тома, задаваемое параметром MAXCAPACITY для класса устройств, составляет 8-16 Гб. Для связанного пула хранения рассмотрите возможность использования совместного размещения по файловым пространствам. Каждая виртуальная машина, для которой создается резервная копия, представлена на сервере IBM Spectrum Protect отдельным файловым пространством. Совместное размещение по файловым пространствам сохраняет данные нескольких операций инкрементного копирования для данной виртуальной машины на одном и то же томе (дисковом файле). При переносе на ленту совместное размещение в файловом пространстве позволяет найти несколько инкрементных резервных копий для данной виртуальной машины на физической ленте в одном месте.

Задать значение режима ленты можно в диалоговом окне **Параметры**.

Резервное копирование прерывается, если для монтирования или быстрого восстановления требуется то же ленточное устройство хранения, которое

используется операцией резервного копирования.

Конфигурирование устройства iSCSI в системе Linux вручную

Linux

Эта процедура описывает, как сконфигурировать систему Linux, используемую во время операции монтирования iSCSI. Снимок виртуальной машины монтируется из хранилища сервера IBM Spectrum Protect.

Прежде чем начать

Во время монтирования iSCSI назначение iSCSI создается в системе агента восстановления. Инициатор Microsoft iSCSI не требуется в системе агента восстановления.

Совет: Инициатор Open-iSCSI поставляется с Red Hat Enterprise Linux и SUSE Linux Enterprise Server.

Перед выполнением этой задачи проверьте, выполнены ли следующие требования iSCSI:

- Можно соединиться с назначением iSCSI с любого компьютера, чтобы создать том, содержащий резервные данные. Этот том можно смонтировать с другого компьютера.
- На любом компьютере, который должен соединяться с назначением iSCSI, требуется инициатор iSCSI.
- На компьютере, на котором нужно восстановить данные, нужно установить инициатор iSCSI.
- Если том находится на нескольких дисках, то нужно смонтировать все нужные диски. Если используются зеркалированные тома, то нужно смонтировать только один из зеркалированных дисков. Монтирование одного диска предотвращает выполнение синхронизации, которая занимает много времени.

Об этой задаче

Выполните эти шаги, чтобы сконфигурировать систему Linux, используемую во время операции монтирования iSCSI:

Процедура

1. Запишите имя инициатора iSCSI на компьютере, на котором нужно восстановить данные. Имя инициатора iSCSI находится в файле `/etc/iscsi/initiatorname.iscsi`. Если значение `InitiatorName=` пустое, то создайте имя инициатора следующей командой:

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   Пример имени инициатора:

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. Добавьте имя инициатора в файл `/etc/iscsi/initiatorname.iscsi`.
   a. Измените файл `/etc/iscsi/initiatorname.iscsi` командой **vi**. Например:

      ```
      twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
      ```

   b. Замените значение параметра **InitiatorName=** на имя инициатора. Например:

      ```
      InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
      ```

3. На компьютере, на котором установлен агент восстановления (или назначение iSCSI), сделайте следующее:
   a. Запустите модуль агент восстановления. Введите данные в окна Выберите сервер IBM Spectrum Protect и Выберите снимок и нажмите **Монтировать**.
   b. В окне Выберите назначение монтирования выберите Смонтировать назначение iSCSI.
   c. Создайте имя назначения. Убедитесь, что оно уникально и что вы можете идентифицировать его с компьютера, на котором работает инициатор iSCSI. Например:

      ```
      iscsi-mount-tsm4ve
      ```

   d. Введите имя инициатора iSCSI, которое вы записали на шаге 1, и нажмите **OK**.
   e. Убедитесь, что смонтированный том показан в поле Смонтированные тома.
4. Найдите и запустите программу инициатора iSCSI на компьютере инициатора, который вы выбрали на шаге 1:
   a. Убедитесь, что служба iSCSI работает, введя следующую команду:
      Red Hat Enterprise Linux:

      ```
      service iscsi status
      ```

      SUSE Linux Enterprise Server:

      ```
      service open-iscsi status
      ```

      Если служба не работает, то запустите ее следующей командой:
      Red Hat Enterprise Linux:

      ```
      service iscsi start
      ```

      SUSE Linux Enterprise Server:

      ```
      service open-iscsi start
      ```

   b. Соединитесь с назначением iSCSI, введя следующую команду:

      ```
      iscsiadm -m discovery -t sendtargets -p <имя хоста/IP
      системы
      агент восстановления> --login
      ```

   c. Убедитесь, что новое устройство raw device доступно:

      ```
      fdisk -l
      ```

5. Смонтируйте файловую систему:
   Для тома не-LVM введите следующую команду. Новое устройство в этом примере: /dev/sdb1:

   ```
   mkdir /mountdir
   mount /dev/sdb1 /mountdir
   ```

   Для тома LVM выполните следующие задачи на госте Linux:
   a. Убедитесь, что на компьютере Linux доступен сценарий vgimportclone. Этот сценарий не поставляется в базовом пакете LVM (пакет по умолчанию). Поэтому обновите пакет LVM до уровня, который содержит этот сценарий.
   b. Введите команду **vgimportclone**, включив в нее новое имя базовой группы томов (VolGroupSnap01). Например:

      ```
      vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
      ```

   c. Введите команду **lvchange**, чтобы пометить логический том как активный. Например:

      ```
      lvchange -a y /dev/VolGroupSnap01/LogVol00
      ```

   d. Введите следующие команды, чтобы смонтировать том:

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. После завершения восстановления файлов введите следующие команды:
   - Для тома не-LVM введите следующую команду:
     a. Размонтировать файловую систему:
        ```
        umount /dev/sdb1 /mountdir
        ```
     b. Удалить том. Если том входит в группу томов, то вначале удалите его из группы томов при помощи следующей команды:
        ```
        vgreduce
        <группа_томов> /dev/sdb1
        ```
        После этого удалите том следующей командой:
        ```
        pvremove /dev/sdb1
        ```
     c. Выйти из одного назначения:
        ```
        iscsiadm --mode node --targetname
        <имя_назначения> --logout
        ```
     d. Выйти из всех назначений:
        ```
        iscsiadm --mode node --logout
        ```
   - Для тома LVM выполните следующие задачи на госте Linux:
     a. Размонтировать файловую систему:
        ```
        unmount /mountdir
        ```
     b. Удалить логический том:
        ```
        lvm lvremove LogVol00
        ```
     c. Удалить группу томов:
        ```
        lvm vgremove VolGroupSnap01
        ```
     d. Выйти из одного назначения:
        ```
        iscsiadm --mode node --targetname
        <имя_назначения> --logout
        ```
     e. Выйти из всех назначений:
        ```
        iscsiadm --mode node --logout
        ```

Конфигурирование устройства iSCSI в системе Windows вручную

Windows

Эта процедура описывает, как сконфигурировать систему Windows, используемую во время операции монтирования iSCSI. Снимок монтируется из хранилища сервера IBM Spectrum Protect.

Прежде чем начать

Перед выполнением этой задачи проверьте, выполнены ли следующие требования iSCSI:

- Во время монтирования iSCSI назначение iSCSI создается на компьютере агент восстановления. Можно соединиться с назначением iSCSI с любого компьютера, чтобы создать том, содержащий резервные данные. Кроме того, после этого можно смонтировать этот том с другого компьютера.
- Инициатор iSCSI требуется на любом компьютере, который должен соединяться с назначением iSCSI.
- На компьютере, на котором нужно восстановить данные, нужно установить инициатор iSCSI.

- Инициатор Microsoft iSCSI не требуется на компьютере агент восстановления.

Перед выполнением этой задачи проверьте, выполнены ли следующие требования диска и тома:

- Если том находится на нескольких дисках, то нужно смонтировать все нужные диски. Если используются зеркалированные тома, то нужно смонтировать только один из зеркалированных дисков. Монтирование одного диска предотвращает выполнение синхронизации, которая занимает много времени.
- Если на компьютере резервного копирования использовалось несколько динамических дисков, то эти диски включаются в одну группу. Поэтому если вы монтируете только один диск, то менеджер дисков Windows может считать, что некоторых дисков нет и выдавать сообщение об ошибке. Игнорируйте это сообщение. Данные на скопированном диске по-прежнему доступны, если только некоторые данные не находятся на другом диске. Эту проблему можно разрешить, смонтировав все динамические диски.

Об этой задаче

Выполните эти задачи, чтобы сконфигурировать систему Windows, используемую во время операции монтирования iSCSI:

Процедура

1. В системе агент восстановления откройте порт `3260` на брандмауэре LAN и брандмауэре клиента Windows. Запишите имя инициатора iSCSI на компьютере, на котором нужно восстановить данные.

   Имя инициатора iSCSI показано в окне Конфигурация инициатора iSCSI в Панели управления. Например:

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. На компьютере, на котором установлен компонент агент восстановления (или объект назначения iSCSI), сделайте следующее:
   a. Запустите графический интерфейс агент восстановления. Введите данные в окна Выберите сервер IBM Spectrum Protect и Выберите снимок и нажмите **Монтировать**.
   b. В окне Выберите назначение монтирования выберите **Смонтировать назначение iSCSI**.
   c. Создайте имя назначения. Убедитесь, что оно уникально и что вы можете идентифицировать его с компьютера, на котором работает инициатор iSCSI. Например:

      ```
      iscsi-mount-tsm4ve
      ```

   d. Введите имя инициатора iSCSI, которое вы записали на шаге 1, и нажмите **OK**.
   e. Убедитесь, что смонтированный том показан в поле Смонтированные тома.
   f. Если вы используете агент восстановления в сети iSCSI и агент восстановления не использует средство перемещения данных, перейдите к файл `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` и задайте тег `[IMOUNT]` и параметр **`Target IP`**:

      ```
      [IMOUNT config]
      Target IP=<IP-адрес сетевой карты на компьютере,
      на котором находятся назначения iSCSI.>
      ```

      Например:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

После добавления или изменения параметра Target IP перезапустите графический интерфейс или интерфейс командной строки Recovery Agent.

3. Найдите и запустите программу инициатора iSCSI на компьютере инициатора, который вы выбрали на шаге 1:
   a. Соединитесь с назначением iSCSI:
      1) На вкладке Назначения введите адрес TCP/IP компонента агент восстановления (назначение iSCSI), который использовался на шаге 2 в окне Назначение:. Щелкните по **Экспресс-соединение**.
      2) В окне Экспресс-соединение показано назначение, соответствующее имени назначения, которое указано на шаге 2c. Если соединение еще не установлено, то выберите это назначение и щелкните по **Соединиться**.
   b. На компьютере инициатора перейдите в **Панель управления > Администрирование > Управление компьютером > Запоминающие устройства > Управление дисками**.
      1) Если смонтированное назначение iSCSI показано как Type=Foreign, то щелкните правой кнопкой мыши по **Foreign Disk** и выберите **Import Foreign Disks**. Выбрано Foreign Disk Group. Щелкните по **OK**.
      2) На следующем экране показаны тип, состояние и размер диска Foreign Disk. Нажмите **OK** и подождите, пока диск не будет импортирован.
      3) По завершении импорта диска нажмите **F5** (обновить). Будет показан смонтированный снимок iSCSI, содержащий назначенную букву диска. Если буквы дисков не назначаются автоматически, то щелкните правой кнопкой мыши по нужному разделу и выберите **Изменить букву диска или путь к диску**. Нажмите **Добавить** и выберите букву диска.
4. Откройте Проводник Windows или другую утилиту, и найдите смонтированный снимок для восстановления файлов.
5. После того, как файл восстановлен, сделайте следующее:
   a. Отсоедините каждое назначение iSCSI, используя окно Свойства инициатора iSCSI.
   b. Размонтируйте том, смонтированный на шаге 2: выберите том в графическом интерфейсе компонента агент восстановления и щелкните по **Размонтировать**.

Конфигурирование прокси-узлы монтирования вручную в системе Linux

Linux

Выполните эту задачу, чтобы добавить прокси-узел монтирования на удаленный компьютер Linux.

Прежде чем начать

В стандартной среде компонента Графический интерфейс Data Protection for VMware vSphere для каждого объекта прокси-узел монтирования используется отдельный раздел файла `dsm.sys`. Все указанные ниже действия выполняются с использованием средства перемещения данных, установленного на сервере резервного копирования.

Об этой задаче

Эта задача настраивает компонент прокси-узлы монтирования, обновляя опции перемещения данных и проверяя соединение с сервером IBM Spectrum Protect.

Процедура

1. Задайте эти опции в файле `dsm.sys`, в разделе прокси-узел монтирования.

   NODENAME
   Задайте имя ранее заданного узла прокси-узел монтирования. Расписания IBM Spectrum Protect связаны с этим узлом.

   PASSWORDACCESS
   Задайте GENERATE, чтобы пароль генерировался автоматически (вместо запроса пользователя).

   MANAGEDSERVICES
   Задайте эту опцию, чтобы указать акцептору клиента, что нужно управлять как веб-клиентом, так и планировщиком (`schedule webclient`).

   TCPSERVERADDRESS
   Задайте адрес TCP/IP для сервера IBM Spectrum Protect.

   TCPPORT
   Задайте адрес порта TCP/IP для сервера IBM Spectrum Protect.

   COMMMETHOD
   Задайте метод связи, который будет использоваться сервером IBM Spectrum Protect. Для объектов прокси-узлы монтирования нужно в качестве метода связи задать TCP/IP. Если задан другой метод, то операции работать не будут.

   HTTPPORT
   Эта опция задает порт TCP/IP и требуется, только если используется несколько служб Client Acceptor (CAD). Например, если есть два узла компонента прокси-узлы монтирования (и две службы CAD), в файле опций для каждого узла компонента прокси-узел монтирования должно быть задано свое значение `HTTPPORT`.

   Ограничение: Не включайте опцию работы без локальной сети (`ENABLELANFREE YES`) в файле `dsm.sys`. Для узлов прокси монтирования эта опция не поддерживается.
   Ниже приведен пример файла dsm.sys с этими параметрами:

```
Servername     tsm_server1
  NODename datacenter1_MP_LNX
  PASSWORDAccess              generate
  MANAGEDServices schedule webclient
  TCPServeraddress tsmserver.myco.com
  TCPPort                     1500
  COMMMethod tcpip
  HTTPPORT 1583
```

2. Введите следующую команду, чтобы задать пользователя и пароль vCenter VMware для компонента прокси-узел монтирования:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <администратор> <пароль1>`
3. Запустите сеанс командной строки перемещения данных с использованием параметров командной строки `-asnodename` и `-optfile`:
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   Убедитесь, что после начального входа в систему у вас не запрашивают пароль.

Внимание: Во избежание сбоя планировщика IBM Spectrum Protect убедитесь, что опция asnodename не задана в разделе файле dsm.sys (Linux). Планировщик запрашивает на сервере IBM Spectrum Protect расписания, связанные с nodename (прокси-узел монтирования), а не с asnodename (узел центра данных). Если в файле dsm.sys задана опция asnodename, то запрашиваются расписания, связанные с asnodename, а не с nodename. В результате операции расписания завершаются неудачно.

4. Проверьте соединение с сервером IBM Spectrum Protect: введите команду
   dsmc query session
   Эта команда выводит информацию о сеансе, включая текущее имя узла, время установления сеанса, информацию о сервере и о соединении с сервером.
5. Настройте службу акцептора (приемника) клиента (Client Acceptor Service, CAD) и службу планировщика перемещения данных, выполнив следующие задачи:
   - Задайте следующие опции в файле dsm.sys, в разделе прокси-узел монтирования:
     – Задайте опцию managedservices со следующими двумя параметрами:
       managedservices schedule webclient

       Эта опция указывает, что демон Client Acceptor управляет и веб-клиентом, и планировщиком.
     – Если вы хотите направлять информацию о расписании и ошибках в файлы журнала не по умолчанию, то задайте опции schedlogname и errorlogname. Каждая опция должна содержать полное имя файла, в котором будет храниться информация журнала. Например:
       schedlogname /vmsched/dsmsched_mp_lnx.log
       errorlogname /vmsched/dsmerror_mp_lnx.log
   - Чтобы сконфигурировать службу акцептора клиента и службу планировщика перемещения данных, так чтобы они работали как сервер резервного копирования, задайте в файле /etc/init.d/dsmcad следующую переменную среды:
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   - Запустите службу Client Acceptor:
     Программа установки создает сценарий запуска демона Client Acceptor Daemon (dsmcad) в /etc/init.d. Демон Client Acceptor Daemon должен быть запущен, чтобы он мог управлять операциями планировщика или веб-клиентом. Введите как пользователь root следующую команду, чтобы запустить демон:
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     service dsmcad start

     Чтобы демон Client Acceptor Daemon запускался автоматически после перезапуска системы, добавьте в окне приглашения оболочки следующую службу:
     # chkconfig --add dsmcad
6. Убедитесь, что акцептор и агент клиента сконфигурированы правильно:
   a. Войдите в удаленную систему.
   b. Соединитесь с компьютером HOST1 при помощи веб-браузера, используя следующие адрес и порт:
      http://HOST1.xyz.yourcompany.com:1581

Конфигурирование прокси-узлы монтирования вручную в удаленной системе Windows

Windows

Выполните эту задачу, чтобы добавить прокси-узел монтирования на удаленный компьютер Windows. Это нужно, если вы хотите добавить в среду второй прокси-узел монтирования Windows.

Прежде чем начать

Прежде чем приступать к этой задаче, убедитесь, что основной компонент прокси-узел монтирования Windows сконфигурирован.

Об этой задаче

Выполните на удаленном прокси-компьютере монтирования Windows следующие действия:

Процедура

1. Установите на удаленном прокси-компьютере монтирования Windows следующие продукты:
   - агент восстановления
   - Средство перемещения данных IBM Spectrum Protect

   Получите доступ к обоим продуктам в образе скачивания IBM Spectrum Protect for Virtual Environments. Пошаговые инструкции по установке смотрите в Центре знаний IBM:
   “Установка Data Protection for VMware в системах Windows” на стр. 26
2. Извлеките контент примера файла опций с созданного прокси-узла монтирования Windows и добавьте его в файл опций на удаленном прокси-компьютере монтирования Windows:
   a. Перейдите на основном прокси-компьютере монтирования Windows в окно Конфигурация модуля Графический интерфейс Data Protection for VMware vSphere.
   b. Щелкните по **Изменить конфигурацию TSM** в списке Задачи. Для загрузки блокнота конфигурации может понадобиться несколько минут.
   c. Перейдите на страницу Смонтировать пары прокси-узлов монтирования.
   d. В столбце таблицы Основной узел перейдите к прокси-узлу монтирования Windows в ожидаемом положении и и щелкните по **Посмотреть параметры**.
   e. Скопируйте пример контента файла `dsm.opt`, показанный в окне **Параметры прокси монтирования**.
   f. Вставьте или добавьте контент примера файла `dsm.opt` в файл опций на удаленном прокси-компьютере монтирования Windows. Присвойте имя файлу опций, следуя правилу, когда указывается его роль как удаленного объекта прокси-узел монтирования.
   Например, `dsm.REMOTE1_MP_WIN.opt`.

   Ограничение: Не включайте опцию работы без локальной сети (`ENABLELANFREE YES`) в файле опций. Для узлов прокси монтирования эта опция не поддерживается.

3. Введите следующую команду средства перемещения данных, чтобы задать пользователя и пароль vCenter VMware для компонента прокси-узел монтирования:

   Совет: Чтобы открыть командную строку dsmc, откройте меню **Пуск Windows** и выберите **Программы → IBM Spectrum Protect → Командная строка клиента резервного копирования**.

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <администратор> <пароль>
   -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

4. Проверьте соединение с сервером IBM Spectrum Protect: введите команду

   ```
   dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

   Эта команда выводит информацию о сеансе, включая текущее имя узла, время установления сеанса, информацию о сервере и о соединении с сервером.

5. Настройте службу акцептора (приемника) клиента (Client Acceptor Service, CAD) и службу планировщика перемещения данных, выполнив следующие шаги:
   На этом шаге для настройки служб CAD и Scheduler используется мастер конфигурирования графического интерфейса клиента IBM Spectrum Protect. По умолчанию служба Remote Client Agent также настраивается в этом мастере. Если вы используете утилиту конфигурирования клиентской службы IBM Spectrum Protect, (`dsmcutil`) для этой задачи, установите также службу агента удаленного клиента.
   Запустите мастер конфигурирования клиента IBM Spectrum Protect из меню Файл: перейдите в **Утилиты > Мастер настройки**:

   a. Выберите `Сконфигурировать веб-клиент TSM`. Введите нужные данные.

      1) Для опции `Когда вы хотите запустить службу?` выберите `Автоматически при загрузке Windows`.
      2) Для опции `Запустить службу по завершении работы этого мастера?` выберите `Да`.

      Когда операция будет успешно выполнена, вернитесь на начальную страницу мастера и перейдите к шагу b.

      Совет: Если вы конфигурируете на одном компьютере более одного объекта прокси-узел монтирования, для каждого экземпляра акцептора клиента нужно задать свой номер порта.

   b. Выберите `Сконфигурировать планировщик клиента TSM`. Введите нужные данные.

      1) При вводе имени планировщика убедитесь, что выбрана опция `Использовать для управления планировщиком Client Acceptor Daemon (CAD)`.
      2) Для опции `Когда вы хотите запустить службу?` выберите `Автоматически при загрузке Windows`.
      3) Для опции `Запустить службу по завершении работы этого мастера?` выберите `Да`.

6. Убедитесь, что акцептор и агент клиента сконфигурированы правильно. Соединитесь с компьютером `HOST1` при помощи веб-браузера, используя следующие адрес и порт:

   `http://HOST1.xyz.yourcompany.com:1581`

Конфигурирование нескольких служб приемника клиента вручную в системе Linux

При определенных обстоятельствах может оказаться выгодным использовать несколько служб dsmcad на одном хосте клиента Linux.

Об этой задаче

Ниже описано, как задать несколько экземпляров dsmcad для автоматического запуска при запуске системы:

Процедура

1. Создайте в файле dsm.sys два уникальных раздела узлов (по умолчанию этот файл находится в каталоге /opt/tivoli/tsm/client/ba/bin/):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod                  TCPip
  TCPPort                     1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess  generate

SErvername node2
  COMMMethod                  TCPip
  TCPPort                     1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess  generate
```

   Совет: Имеет смысл включить некоторые опции include/exclude, чтобы различить эти узлы. В ином случае одни и те же данные могут быть скопированы с использованием двух имен узлов.

2. Создайте два файла dsm.opt, по одному для каждого узла (по умолчанию эти файлы находятся в каталоге /opt/tivoli/tsm/client/ba/bin):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Разрешите опцию passwordaccess generate, войдя в систему с идентификационными данными для обоих узлов:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Создайте две копии сценария инициализации rc.dsmcad (по умолчанию этот сценарий находится в каталоге /opt/tivoli/tsm/client/ba/bin):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Измените rc.dsmcad-node1:
   a. Измените эту строку для дистрибутивов Red Hat Enterprise Linux:

      ```
      daemon $DSMCAD_BIN
      ```

      на строку

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

   b. Измените эту строку для дистрибутивов SUSE Linux Enterprise Server:

      ```
      startproc $DSMCAD_BIN
      ```

      на строку

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

6. Измените rc.dsmcad-node2:
   a. Измените эту строку для дистрибутивов Red Hat Enterprise Linux:

      ```
      daemon $DSMCAD_BIN
      ```

      на строку

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

   b. Измените эту строку для дистрибутивов SUSE Linux Enterprise Server:

      ```
      startproc $DSMCAD_BIN
      ```

      на строку

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

7. Создайте в `/etc/init.d/` ссылки, указывающие на два новых сценария инициализации rc.dsmcad. Эти ссылки позволяют службе инициализации Linux запускать службы dsmcad при запуске системы:

   ```
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
   # ls -la dsm*
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
   ```

8. Зарегистрируйте два новых сценария rc посредством **`chkconfig`**:

   ```
   # chkconfig --add dsmcad-node1
   # chkconfig --add dsmcad-node2
   ```

9. Проверьте конфигурацию при помощи команды **`service dsmcad start`**, чтобы убедиться, что сценарии загружаются и запускаются без проблем:

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

В этом примере текст команды размещен в двух строках (в соответствии с форматированием страницы).

10. Перезапустите систему и убедитесь, что два экземпляра dsmcad запускаются автоматически:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

В этом примере текст команды размещен в двух строках (в соответствии с форматированием страницы).

Изменение файла конфигурации VMCLI

Файл конфигурации VMCLI (`vmcliConfiguration.xml`) содержит параметры для компонента Графический интерфейс Data Protection for VMware vSphere.

Процессу установки Data Protection for VMware требуется, чтобы пользователь задал IP-адрес сервера vCenter, а также указал, нужно ли включить доступ к графическому интерфейсу для веб-браузера. Однако после установки программа установки не сможет изменить IP-адрес сервера и метод доступа графического интерфейса.

Чтобы обновить эти параметры, можно вручную внести изменения в файл конфигурации VMCLI (`vmcliConfiguration.xml`). Этот файл создается при установке в следующих расположениях:
В системах Windows:
`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
В системах Linux:
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

Чтобы изменить опцию, указывающую, нужно ли включить доступ к графическому интерфейсу через веб-браузер, введите одно из следующих значений в параметр **<enable_direct_start></enable_direct_start>**.

- *yes* Веб-браузер сможет непосредственно получить доступ к графическому интерфейсу. Например:

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* Веб-браузер не сможет непосредственно получить доступ к графическому интерфейсу. Например:

```
<enable_direct_start>no</enable_direct_start>
```

Чтобы использовать графический интерфейс для защиты vSphere, задайте следующее значение в параметре **<mode></mode>**:

- *vcenter* Для защиты vSphere используется графический интерфейс. Например:

```
<mode>vcenter</mode>
```

Чтобы изменить IP-адрес сервера vCenter, убедитесь, что задано **<mode>vcenter</mode>**, а затем укажите IP-адрес в параметре **<vcenter_url></vcenter_url>**. Например:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

В начале IP-адреса сервера vCenter должно находиться значение `https://`. В конце IP-адреса сервера vCenter должно находиться значение `/sdk`.

Пример файлов `vmcliConfiguration.xml`

Следующий файл `vmcliConfiguration.xml` сконфигурирован для защиты vSphere, и для графического интерфейса включен доступа через веб-браузер:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcenter</mode>
 <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Приложение B. Перенастройка до стратегии инкрементного резервного копирования Всегда инкрементное

Используйте эту процедуру, чтобы перенастроить существующих расписания резервного копирования, политики и объекты узел перемещения данных для использования в стратегии резервного копирования Всегда инкрементное.

Прежде чем начать

Вы можете использовать стратегию полного резервного копирования Всегда инкрементное, реализованную в Data Protection for VMware версии 6.2 и 6.3. Если вы хотите продолжить использовать стратегию полного резервного копирования Всегда инкрементное, вам не нужно изменять политику или расписания. Вы должны убедиться, что обновляете только узлы перемещения данных до версии 6.4 (или новее), как описано в следующей процедуре. Однако, если вы хотите использовать стратегию инкрементного резервного копирования Всегда инкрементное, вы должны, помимо обновления узлов перемещения данных до версии 6.4 (или новее), также обновить расписания и политику для тех узлов перемещения данных, которые переходят в эту стратегию инкрементного резервного копирования Всегда инкрементное.

Чтобы перенастроить существующие расписания Data Protection for VMware в стратегию инкрементного резервного копирования Всегда инкрементное, нужно выполнить задачи, описанные в этой процедуре.

Важное замечание:

- Хотя некоторые задачи являются отдельными, все приложения и компоненты нужно в конечном счете обновить, чтобы получить полный набор преимуществ стратегии инкрементного резервного копирования Всегда инкрементное. В этой публикации содержится вся информация по выполнению каждой задачи.
- Есть несколько методов выполнения всей перенастройки. Однако в этой публикации описаны эффективные методы для типичной среды Data Protection for VMware.
- Расписание, которое нужно перенастроить в этой процедуре - это расписание, созданное с помощью мастера резервного копирования Графический интерфейс Data Protection for VMware vSphere. Если перенастраиваемое расписание создано вручную, то все описанные здесь изменения также нужно выполнить вручную.

Об этой задаче

Процедура

1. Обновите все серверы резервного копирования vStorage, которые защищают один vCenter. Это обновление нужно выполнить одновременно для всех узлов перемещения данных.
   - При этом обновлении нужно установить средство перемещения данных IBM Spectrum Protect версии 6.4 (или новее) на сервере резервного копирования vStorage.
   - Это отдельная задача, поэтому выполнять шаги 2 или 3 сразу после шага 1 необязательно. После обновления узлов перемещения данных можно

по-прежнему выполнять резервное копирование виртуальных машин в существующей среде. Шаги 2 и 3 можно выполнить в более удобное время.

Совет: Если среда содержит несколько серверов резервного копирования vStorage, то обновите только один сервер. Перед обновлением остальных серверов резервного копирования vStorage убедитесь, что этот сервер работает нормально.

2. Обновите политику резервного копирования и расписания резервного копирования, чтобы реализовать операции инкрементного резервного копирования Всегда инкрементное:
   Выполните следующие операции для политики резервного копирования на сервере IBM Spectrum Protect, вводя команды в клиенте командной строки администрирования (`dsmadmc`):
   a. Создайте класс управления для соответствующего домена и набор политики для инкрементных резервных копий Всегда инкрементное. В следующем примере создается класс управления `mgmt_ifincr28` для домена `domain1` и набора политик `prodbackups`. Имя класса управления используется для описания стратегии инкрементного резервного копирования Всегда инкрементное, при котором сохраняется 28 версий резервных копий:

      ```
      define mgmtclass domain1 prodbackups mgmt_ifincr28
      description="Retain 28 backup versions"
      ```

   b. Создайте группу резервных копий для инкрементных резервных копий Всегда инкрементное. В этом примере создается стандартная группа резервных копий для домена `domain1`, набора политик `prodbackups` и класса управления `mgmt_ifincr28`:

      ```
      define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
      ```

      Записи `standard type=backup` - это значения по умолчанию, и их можно не задавать. Они включены в этот пример, чтобы показать, что имя группы копий - `STANDARD`, а тип резервного копирования - `backup`, а не `archive`.

   c. Измените группу резервных копий, указав подходящие версию, срок хранения и параметры устаревания:

      Напоминание: В Data Protection for VMware версии 6.2 и 6.3 версия резервной копии, срок хранения и срок окончания действия основаны на уровне детализации цепи резервных копий. Этот метод означает, что даже хотя и создаются полные резервные копии Всегда инкрементное и инкрементные резервные копии Всегда инкрементное (как часть стратегии полного резервного копирования Всегда инкрементное 6.2 и 6.3), окончание действия версий учитывает только полные резервные копии. В Data Protection for VMware версии 6.4 (или новее) версии резервных копий, срок хранения и срок окончания действия основаны на уровне детализации одной резервной копии. Этот метод означает, что учитывается окончание действия версий как для полных резервных копий Всегда инкрементное, так и для инкрементных резервных копий Всегда инкрементное.

      Параметр `verexists` задает максимальное число версий резервных копий виртуальной машины, сохраняемых на сервере. Если операция инкрементного резервного копирования Всегда инкрементное вызывает превышение этого числа, сервер сочтет срок действия наиболее старой версии резервной копии, находящейся в серверном хранилище, истекшим. В этом примере задано `verexists=28`. Это значит, что на сервере хранится не больше 28 версий резервных копий виртуальной машины.

      Параметр `retextra` задает максимальное число дней для хранения версии резервной копии виртуальной машины; по истечении этого времени версия становится неактивной. В этом примере задано `retextra=nolimit`. Это значит,

что максимальное число неактивных версий резервных копий хранится неопределенно долго. Однако если задано `verexists`, то значение `nolimit` заменяется значением `verexists`. В результате в этом примере на сервере хранится не больше 28 неактивных версий резервных копий виртуальной машины.

На основе параметров, описанных в этом шаге, группа резервных копий изменяется следующим образом:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

В этом примере существующая среда Data Protection for VMware версии 6.3 состоит из следующих хостов и расписаний:

- Кластер ESX (`esxcluster`), который содержит два хоста ESX (`esxhost1`, `esxhost2`).
- Расписание `bup_esxcluster_full` запускает еженедельное полное резервное копирование Всегда инкрементное для каждого хоста ESX со средством перемещения данных `dm1`.
- Расписание `bup_esxcluster_incr` запускает ежедневное инкрементное резервное копирование Всегда инкрементное для каждого хоста ESX со средством перемещения данных `dm2`.

Выполните в Графический интерфейс Data Protection for VMware vSphere следующие задачи планирования резервного копирования:

a. Запустите модуль Графический интерфейс Data Protection for VMware vSphere, щелкнув по значку в окне Решения и приложения клиента vSphere.

b. Щелкните в окне Начинаем работу по вкладке **Резервное копирование**, чтобы открыть окно Управление расписаниями резервного копирования.

c. Найдите расписание резервного копирования (используемое для полных или инкрементных резервных копий Всегда инкрементное), чтобы его обновить. В этой процедуре используется расписание полного резервного копирования Всегда инкрементное, `bup_esxcluster_full`.

d. Щелкните правой кнопкой мыши по расписанию и выберите **Свойства**.

e. Перейдите на страницу Расписание и выберите **Инкрементное** в раскрывающемся списке **Стратегия резервного копирования**.

f. Нажмите **ОК**, чтобы сохранить обновления.

g. Найдите расписание резервного копирования, используемое для инкрементных резервных копий Всегда инкрементное. Щелкните правой кнопкой мыши по расписанию и выберите **Удалить**. Поскольку расписание полного резервного копирования Всегда инкрементное, `bup_esxcluster_full`, обновлено до инкрементного резервного копирования Всегда инкрементное, это расписание инкрементного резервного копирования Всегда инкрементное больше не требуется.

3. Теперь, когда у вас есть расписание инкрементного резервного копирования Всегда инкрементное, вы можете сократить число узлов перемещения данных, консолидировав их:
В этом примере два узла перемещения данных объединяются в один.

a. Откройте на сервере резервного копирования vStorage командную строку и перейдите в каталог, в котором находится файл опций для `dm1`.

b. Откройте файл в редакторе текстов (например, Блокнот) и задайте в файле следующие опции:

1) Задайте `vmmaxparallel`, чтобы указать число виртуальных машин, копируемых одновременно узлом `dm1`:

```
vmmaxparallel=2
```

Значение по умолчанию и минимальное значение - 1. Максимальное значение - 50.

Совет: Для каждого удаляемого узла перемещения данных увеличьте значение `vmmaxparallel` на 1.

Можно также задать `vmlimitperhost`, чтобы указать число виртуальных машин, копируемых одновременно узлом `dm1` с одного хоста ESX:

```
vmlimitperhost=1
```

Это опция полезна, если вы хотите защитить хост от перегрузки. Значение по умолчанию - 0 (нет ограничений). Минимальное значение - 1. Максимальное значение - 50.

c. Войдите на сервер IBM Spectrum Protect. Задайте в клиенте командной строки администрирования (`dsmadmc`) максимальное число сеансов резервного копирования виртуальной машины для соединения с хостом. Например:

```
maxsessions=4
```

Значение по умолчанию - 25. Минимальное значение - 2.

4. Убедитесь, что измененные узлы перемещения данных работают правильно:
   a. Запустите модуль Графический интерфейс Data Protection for VMware vSphere, щелкнув по значку в окне Решения и приложения клиента vSphere Client.
   b. Щелкните в окне Начинаем работу по вкладке Конфигурация, чтобы открыть страницу Состояние конфигурации.
   c. На странице Состояние конфигурации выберите vCenter, защищенный на шаге 1. Щелкните по узлу перемещения данных, чтобы просмотреть информацию о состоянии в панели Сведения о состоянии. Если для узла показаны предупреждение или ошибка, щелкните по этому узлу и используйте информацию в панели Сведения о состоянии, чтобы устранить ошибку. После этого выберите узел и щелкните по **Проверить выбранный узел**, чтобы проверить, исправлена ли ошибка. Щелкните по Обновить, чтобы заново протестировать все узлы.

Результаты

После успешного завершения каждой задачи среда будет готова к использованию стратегии инкрементного резервного копирования Всегда инкрементное.

Ограничения: После перенастройки расписаний, относящихся к типу полного резервного копирования Всегда инкрементное, до типа инкрементного резервного копирования Всегда инкрементное помните о следующих ограничениях:

- Изменение перенастроенных расписаний обратно, так чтобы они снова относились к типу полного резервного копирования Всегда инкрементное для VM (файловое пространство), не поддерживается.
- Использование более ранней версии средства перемещения данных IBM Spectrum Protect для перенастроенного файлового пространства не поддерживается.
- Если файловое пространство содержит одну (или более) инкрементных резервных копий Всегда инкрементное, полная резервная копия Всегда инкрементное не поддерживается.

Пример управления версиями при помощи параметра `verexists`

В этом примере перенастройки расписания Data Protection for VMware версии 6.3 использует следующие два расписания резервного копирования:

- `-mode=full`: Планируется еженедельное полное резервное копирование Всегда инкрементное (по воскресеньям), а максимальное число версий резервных копий VM, сохраняемых на сервере, равно четырем (`verexists=4`).
- `-mode=incr`: Запланировано еженедельное инкрементное резервное копирование Всегда инкрементное (с понедельника по субботу).

За 4 недели создается 28 резервных копий:

- Четыре полных резервных копии Всегда инкрементное (по одной полной резервной копии каждую неделю, умноженные на четыре недели)
- 24 инкрементных резервных копии Всегда инкрементное (инкрементные резервные копии за шесть дней, умноженные на четыре недели)

Поскольку Data Protection for VMware версии 6.3 подсчитывает только полные резервные копии, значение `verexists=4` сохраняет все 28 копий.

Чтобы обеспечить такой же уровень защиты с использованием Data Protection for VMware версии 6.4 (или новее) и стратегии инкрементного резервного копирования Всегда инкрементное, создайте следующее расписание:
`-mode=iffull`: Планируется ежедневное полное резервное копирование Всегда инкрементное, и параметру `verexists` присваивается значение 28.
За 4 недели создается 28 резервных копий:

- Одна полная резервная копия Всегда инкрементное (первоначальная резервная копия, умноженная на один день)
- 27 инкрементных резервных копии Всегда инкрементное (ежедневные резервные копии Всегда инкрементное, умноженные на 27 дней)

Поскольку Data Protection for VMware версии 6.4 (или новее) учитывает как полные резервные копии Всегда инкрементное, так и инкрементные резервные копии Всегда инкрементное, значение `verexists=28` позволяет сохранить все 28 резервных копий.

Приложение C. Специальные возможности для семейства продуктов IBM Spectrum Protect

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

Обзор

Продукты семейства IBM Spectrum Protect поддерживают следующие основные специальные возможности:

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

Семейство продуктов IBM Spectrum Protect использует новейший стандарт W3C, WAI-ARIA 1.0(www.w3.org/TR/wai-aria/), чтобы обеспечить соответствие разделу US Section 508(www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) и рекомендациям по доступности веб-содержимого (Web Content Accessibility Guidelines (WCAG) 2.0(www.w3.org/TR/WCAG20/). Чтобы воспользоваться преимуществами специальных возможностей, возьмите последний выпуск вашей программы чтения информации с экрана и последний веб-браузер, поддерживаемый продуктом.

Документация по продукту в центре знаний IBM включена для поддержки специальных возможностей. Специальные возможности центра знаний IBM описаны в разделе Специальные возможности справки по центру знаний IBM (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Управление при помощи клавиатуры

Для управления этим продуктом используются стандартные комбинации клавиш.

Информация об интерфейсе

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

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

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

Программное обеспечение поставщиков

В семейство продуктов IBM Spectrum Protect включены программы некоторых поставщиков, на которые не распространяется лицензионное соглашение IBM. IBM не делает никаких заявлений относительно специальных возможностей этих продуктов.

За информацией о специальных возможностях этих продуктов обращайтесь к их поставщикам.

Связанная информация о специальных возможностях

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

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

Дополнительную информацию об обязательствах, которые IBM принимает на себя в отношении поддержки специальных возможностей, смотрите на сайте IBM Accessibility (IBM - Специальные возможности) (www.ibm.com/able).

Замечания

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ЛИЦЕНЗИЯ НА ПРАВО КОПИРОВАНИЯ:

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

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

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

Товарные знаки

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

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

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

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

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

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

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

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

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

Положения и условия для документации по продукту

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

Применимость

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

Личное использование

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

Коммерческое использование

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

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

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

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

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

Замечания о политике конфиденциальности

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

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

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

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

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

Глоссарий

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

См. IBM Spectrum Protect - Глоссарий.

Индекс

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Номер программы: 5725-X00

Напечатано в Дании