Dell EMC PowerStore

Руководство по настройке системы безопасности

1.x

July 2020
Ред. A02

Примечания, предупреждения и предостережения

ПРИМЕЧАНИЕ: Пометка ПРИМЕЧАНИЕ указывает на важную информацию, которая поможет использовать данное изделие более эффективно.

ОСТОРОЖНО: Указывает на возможность повреждения устройства или потери данных и подсказывает, как избежать этой проблемы.

ПРЕДУПРЕЖДЕНИЕ: Указывает на риск повреждения оборудования, получения травм или на угрозу для жизни.

Содержание

Предисловие

Для улучшения продуктов периодически выпускаются обновленные версии программного обеспечения и оборудования. Некоторые функции, описанные в этом документе, поддерживаются не всеми версиями программного обеспечения или оборудования, которые используются на данный момент. Примечания к выпуску продукта содержат последние обновленные сведения о функциях продукта. Если продукт не работает должным образом либо работает не так, как описано в этом документе, обратитесь к специалистам службы технической поддержки.

Ресурсы поддержки

Информацию о продуктах, их поддержке и лицензировании можно получить перечисленными ниже способами.

- **Сведения о продуктах**

  Для изучения документации по продуктам и функциям, а также примечаний к выпускам, перейдите на PowerStore Страницу документации по адресу www.dell.com/powerstoredocs.

- **Поиск и устранение неисправностей**

  Для получения информации о продуктах, обновлениях ПО, лицензировании и сервисном обслуживании перейдите на сайт www.dell.com/support и найдите страницу поддержки для соответствующего продукта.

- **Техническая поддержка**

  Для получения технической поддержки и оформления сервисных заявок перейдите на www.dell.com/support страницу **Сервисные заявки**. Чтобы подать сервисную заявку, необходимо иметь действующее соглашение о поддержке. Для получения сведений о порядке заключения соглашения о поддержке, а также по любым вопросам, связанным с вашей учетной записью, обращайтесь к менеджеру по продажам.

1

Аутентификация и доступ

В этой главе содержится следующая информация:

Темы:

Аутентификация и управление учетными записями пользователей, ролями и привилегиями

Аутентификация для предоставления доступа к кластеру выполняется по учетным данным учетной записи пользователя. Для создания учетных записей пользователей и управления ими используется страница **Users**, для доступа к которой в PowerStore Manager необходимо выбрать **Settings** > **Users** > **Users**. Разрешения зависят от роли, связанной с учетной записью пользователя. Когда пользователь указывает в веб-браузере сетевой адрес кластера в виде URL-адреса, открывается страница входа, которая позволяет пользователю пройти аутентификацию в качестве локального пользователя. Введенные пользователем учетные данные пройдут аутентификацию, после чего в системе будет создана сессия. В дальнейшем пользователь может осуществлять мониторинг кластера и управлять им в рамках назначенной пользователю роли.

Кластер аутентифицирует своих пользователей, проверяя их имена и пароли с помощью безопасного соединения с сервером управления.

Заводские возможности управления, заданные по умолчанию

Устройство поставляется с заводскими параметрами учетных записей пользователей по умолчанию, которые предназначены для первого входа в систему на устройстве и его начальной настройки.

ПРИМЕЧАНИЕ: Начальную настройку PowerStore выпусков 1.0.x рекомендуется производить с помощью пользовательского интерфейса PowerStore Manager. Программный интерфейс API, интерфейс командной строки или интерфейс сервисных скриптов использовать не рекомендуется. В этом случае все пароли по умолчанию будут гарантированно изменены.

Тип учетной записи	Имя пользователя	Пароль	Права
Управление системой	admin	Password123#	Привилегии администратора для сброса паролей по умолчанию, настройки параметров

Тип учетной записи	Имя пользователя	Пароль	Права
			устройства и управления учетными записями пользователей.
Обслуживание	service	service	Для выполнения сервисных операций. **ПРИМЕЧАНИЕ:** Сервисный пользователь существует для доступа с помощью протокола безопасной оболочки (SSH). Однако нельзя войти в PowerStore Manager, используя учетную запись сервисного пользователя.

Правила сессий

Сессии в кластере обладают следующими характеристиками:

- срок их действия истекает через один час;
  ПРИМЕЧАНИЕ: Пользователь автоматически выходит из кластера, если сессия была неактивной в течение одного часа.
- настройка времени ожидания сессии не предусмотрена;

Использование имени пользователя и пароля

Имена пользователей системных учетных записей должны соответствовать следующим требованиям:

Ограничение	Требования к имени пользователя
Структура	Должно начинаться и заканчиваться буквенно-цифровым символом.
Регистр	Регистр символов в именах пользователей не учитывается.
Минимальное количество буквенно-цифровых символов	1
Максимальное количество буквенно-цифровых символов	64
Поддерживаемые специальные символы	. (точка)

Пароли системных учетных записей должны соответствовать следующим требованиям:

Ограничение	Требования к паролю
Минимальное количество символов	8
Минимальное количество символов верхнего регистра	1
Минимальное количество символов нижнего регистра	1
Минимальное количество цифровых символов:	1
Минимальное количество специальных символов • Поддерживаемые символы: ! @ # $ % ^ * _ ~ ? **ПРИМЕЧАНИЕ:** Пароль не может содержать одинарные кавычки ('), амперсанд (&) и пробел.	1
Максимальное количество символов	40

ПРИМЕЧАНИЕ: Последние пять паролей блокируются, чтобы их нельзя было использовать повторно. Предыдущим паролем можно воспользоваться повторно после пяти последовательных смен паролей.

Пароли ESXi

Используемый по умолчанию пароль учетной записи root для ESXi на устройстве PowerStore X model имеет следующий формат: ***<Service_Tag>*_123!**, где *<Service_Tag>* — это семизначный сервисный код Dell для данного устройства.

Не изменяйте пароль ESXi по умолчанию до завершения первоначальной настройки кластера. Дополнительные сведения об изменении пароля ESXi см. в документации по VMware ESXi.

ОСТОРОЖНО: Очень важно не потерять пароль ESXi. Если у вас не будет пароля, когда ESXi выйдет из строя, устройство придется инициализировать повторно. Это нормальная ситуация для ESXi, однако повторная инициализация из-за потери пароля может привести к потере данных.

ОСТОРОЖНО: Пароль ESXi по умолчанию имеет уникальную конфигурацию для каждого устройства PowerStore X model. Пароль используется для аутентификации на хосте ESXi при добавлении узлов устройства в кластер vCenter. Если вы измените пароль по умолчанию до полной настройки кластера, вам потребуется повторно инициализировать устройство.

Роли и права

Контроль доступа на основе ролей позволяет пользователям иметь разные привилегии. В результате этого появляется способ разделения ролей администрирования для обеспечения оптимального соответствия между имеющейся квалификацией и назначаемыми обязанностями.

Система поддерживает следующие роли и привилегии.

ПРИМЕЧАНИЕ: Символ ✓ в ячейке таблицы обозначает поддерживаемую привилегию для этой роли, а пустая ячейка указывает на то, что привилегия для этой роли не поддерживается.

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
Изменение локального пароля системы	✓	✓	✓	✓	✓
Просмотр сведений о настройках, состоянии и производительности системы	✓		✓	✓	✓
Изменение параметров системы					✓
Создание, изменение и удаление ресурсов и политик защиты, а также активация/отключение SSH				✓	✓
Подключение к vCenter		✓		✓	✓
Просмотр списка локальных учетных записей			✓		✓
Добавление, удаление или изменение локальной учетной записи			✓		✓
Просмотр сведений о системном хранилище с помощью сервера vCenter, подключенного к поставщику VASA системы, регистрация и повторная регистрация сертификата источника сертификатов (CA) или		✓			✓

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
источника сертификатов VMware (VMCA)					

Роли и привилегии, связанные с файлами

Система поддерживает следующие роли и привилегии, связанные с файлами.

ПРИМЕЧАНИЕ: Символ ✓ в ячейке таблицы обозначает поддерживаемую привилегию для этой роли, а пустая ячейка указывает на то, что привилегия не поддерживается для этой роли.

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
Просмотрите следующее: • оповещения файловой системы; • список серверов сетевой системы хранения данных (NAS); • список файловых систем; • список пользовательских квот для файлов; • список маршрутов интерфейсов для файлов; • список интерфейсов для файлов; • список сетевых папок SMB; • список операций экспорта NFS.	✓		✓	✓	✓
Просмотрите следующее: • список DNS-серверов для файлов или указанный DNS-сервер; • список FTP-серверов для файлов или указанный FTP-сервер; • список интерфейсов для файлов или указанный интерфейс для файлов; • список маршрутов интерфейсов для файлов или указанный маршрут интерфейса; • список серверов Kerberos для файлов или указанный сервер Kerberos; • список серверов LDAP для файлов или указанный сервер LDAP; • список серверов NDMP для файлов или указанный сервер NDMP;	✓		✓	✓	✓

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
• список серверов NIS для файлов или указанный сервер NIS; • список файловых систем или указанная файловая система; • список квот деревьев для файлов или указанная квота деревьев для файлов; • список квот пользователей для файлов или указанная квота пользователей; • список средств антивирусной проверки для файлов или указанное средство антивирусной проверки для файлов; • список серверов NAS или указанный сервер NAS; • список операций экспорта NFS или указанная операция экспорта NFS; • список серверов NFS или указанный сервер NFS; • список серверов SMB или указанный сервер SMB; • список сетевых папок SMB или указанная сетевая папка SMB.					
Добавление, изменение, удаление или пингование указанного сервера NAS либо отправка пароля, хостов или групп на указанный сервер NAS				✓	✓
Просмотр пароля или хостов указанного сервера NAS			✓		✓
Добавление файловой системы, а также изменение или удаление указанной файловой системы на существующем сервере NAS				✓	✓
Добавление клона или моментального снимка в указанную файловую систему, обновление или восстановление указанной файловой системы либо обновление квоты указанной файловой системы				✓	✓
Добавление квоты деревьев для файлов, а также изменение, удаление или обновление указанной квоты деревьев для файлов				✓	✓

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
Добавление квоты пользователей для файлов, а также изменение, удаление или обновление указанной квоты пользователей для файлов				✓	✓
Добавление средства антивирусной проверки для файлов, изменение или удаление указанного средства антивирусной проверки для файлов либо отправка указанной конфигурации средства антивирусной проверки для файлов					✓
Загрузка указанной конфигурации средства антивирусной проверки для файлов			✓		✓
Добавление сервера SMB или NFS, а также изменение, удаление, присоединение или отсоединение указанного сервера SMB или NFS				✓	✓
Добавление сетевой папки SMB, а также изменение или удаление указанной сетевой папки SMB				✓	✓
Добавление операции экспорта NFS, а также изменение или удаление указанной операции экспорта NFS				✓	✓
Добавление интерфейса для файлов, а также изменение или удаление указанного интерфейса для файлов				✓	✓
Добавление маршрута интерфейса для файлов, а также изменение или удаление указанного маршрута интерфейса для файлов				✓	✓
Добавление сервера DNS для файлов, сервера FTP для файлов, сервера Kerberos для файлов, сервера LDAP для файлов, сервера NDMP для файлов или сервера NIS для файлов, а также изменение или удаление указанного сервера DNS для файлов, сервера FTP для файлов, сервера Kerberos для файлов, сервера LDAP для файлов, сервера NDMP для файлов или сервера NIS для файлов				✓	✓

Задача	Оператор	Администратор виртуальной машины	Администратор безопасности	Администратор хранилища	Администратор
Отправка keytab Kerberos для файлов					✓
Загрузка keytab Kerberos для файлов	✓		✓		✓
Отправка конфигурации LDAP или сертификата LDAP для файлов					✓
Загрузка сертификата LDAP для файлов			✓		✓

Управление учетными записями пользователей на основе привилегий роли

Пользователь с ролью администратора или администратора безопасности может выполнять следующие действия по управлению учетными записями пользователей:

- создавать новые учетные записи пользователей;
- удалять любые учетные записи пользователей, кроме встроенной учетной записи администратора;

  ПРИМЕЧАНИЕ: Встроенную учетную запись администратора удалить невозможно.
- изменять роль другого пользователя на любую другую;
- сбрасывать пароли других пользователей;
- выполнять блокировку и разблокировку других учетных записей пользователей.

  ПРИМЕЧАНИЕ: Вошедшие в систему пользователи с ролью администратора или администратора безопасности не могут заблокировать свою учетную запись.

Вошедшие в систему пользователи не могут удалять собственные учетные записи. Кроме того, за исключением пользователей с ролью администратора или администратора безопасности, вошедшие в систему пользователи могут изменять только свои собственные пароли. Для изменения пароля пользователю необходимо ввести свой старый пароль. Вошедшие в систему пользователи не могут сбрасывать собственные пароли, изменять собственные роли, а также блокировать или разблокировать собственные учетные записи.

Встроенный профиль учетной записи администратора (с ролью администратора) невозможно редактировать и нельзя заблокировать.

Если роль пользователя или состояние блокировки будут изменены, либо пользователь будет удален, либо пароль пользователя будет изменен администратором или администратором безопасности, все сессии, привязанные к этому пользователю, станут недействительными.

ПРИМЕЧАНИЕ: Если пользователи изменяют собственные пароли в ходе сессии, сессия остается активной.

Сброс паролей администратора и сервисной учетной записи

Устройство поставляется с используемой по умолчанию учетной записью пользователя-администратора, позволяющей выполнить начальную настройку. Также в состав системы входит используемая по умолчанию служебная учетная запись пользователя, позволяющая выполнять специальные функции обслуживания. Для начальной настройки PowerStore рекомендуется использовать пользовательский интерфейс PowerStore Manager, а не какой-либо другой способ, например программный интерфейс REST API или интерфейс командной строки. При использовании пользовательского интерфейса PowerStore Manager все пароли по умолчанию будут гарантированно изменены. Если вы забыли новые пароли, можно восстановить значения паролей по умолчанию.

Метод восстановления этих паролей зависит от того, какое устройство вы используете: PowerStore T model или PowerStore X model. Используйте метод, соответствующий типу вашего устройства, чтобы сбросить пароль администратора, пароль сервисной учетной записи или оба пароля сразу.

Восстановление паролей администратора и сервисной учетной записи по умолчанию на устройстве PowerStore T model

Об этой задаче

Для устройства PowerStore T model в качестве основного метода восстановления пароля учетной записи администратора и сервисной учетной записи является использование USB-накопителя. Поддерживаются файловые системы FAT32 и ISO 9660.

ПРИМЕЧАНИЕ: Чтобы восстановить пароль, когда устройство находится в режиме обслуживания, выполните следующие действия с одним отличием. Примените для каждого узла процесс перезапуска по USB. Это действие гарантирует, что после возврата системы в нормальный режим и после входа в PowerStore Manager будет отображаться запрос на ввод нового пароля как для пользователей-администраторов, так и для сервисных пользователей.

Действия

1. Если USB-накопитель отформатирован, перейдите к следующему шагу. Если нет, воспользуйтесь командой в командной строке (например, `format <d:> /FS:FAT32`), чтобы отформатировать накопитель.

   Где `d:` — имя диска для USB-накопителя, вставленного в ноутбук или компьютер.

2. Присвойте метку с помощью команды:

   ```
   label d:
   RSTPWD
   ```

   ПРИМЕЧАНИЕ: Устройство не будет подключать USB-накопитель без метки `RSTPWD`. После присвоения метки USB-накопителю вставьте пустой файл для паролей учетных записей, которые требуется восстановить. Можно сбросить пароль учетной записи администратора, пароль сервисной учетной записи или оба пароля одновременно.

3. Чтобы создать пустой файл на накопителе, воспользуйтесь одной или двумя следующими командами по мере необходимости:

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Вставьте USB-накопитель в USB-порт любого узла устройства, подождите 10 секунд, а затем извлеките его.
   Теперь пароль для каждой учетной записи, который вы восстанавливаете, имеет значение по умолчанию.
5. Подключитесь к кластеру с помощью браузера, используя IP-адрес кластера, и войдите в качестве администратора с первоначальным паролем по умолчанию — **`Password123#`**.
   Отобразится запрос на сброс пароля администратора, пароля сервисной учетной записи или обоих паролей. Чтобы сбросить пароль сервисной учетной записи с помощью протокола безопасной оболочки (SSH), используйте первоначальное значение пароля сервисной учетной записи по умолчанию — **`service`**.
6. Измените значение пароля администратора по умолчанию на пользовательское.
7. Чтобы пароль сервисной учетной записи отличался от пароля администратора, снимите соответствующий флажок.

Результат

Если после выполнения этой процедуры запрос на сброс пароля так и не отобразится при попытке входа в систему, обратитесь к поставщику услуг.

Восстановление паролей администратора и сервисной учетной записи по умолчанию на устройстве PowerStore X model

Предварительные условия

Необходимо знать имя первичного узла главного устройства (например, PSTX-44W1BW2-A и PowerStore D6013). Если требуется, создайте файл `reset.iso`.

Об этой задаче

Для устройства PowerStore X model воспользуйтесь образом ISO, подключив его из vSphere. Предварительно созданные файлы образа можно скачать на странице www.dell.com/support. Можно также создать собственный образ в системе Linux, выполнив одну или обе сенсорные команды в зависимости от того, какие пароли следует восстановить.

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

ПРИМЕЧАНИЕ: Образ ISO, `reset.iso`, необходимо поместить в хранилище данных, прежде чем его можно будет подключить как виртуальный компакт-диск из vSphere.

ПРИМЕЧАНИЕ: Чтобы восстановить пароль, когда устройство находится в режиме обслуживания, выполните следующие действия с двумя отличиями. Во-первых, необходимо загрузить образ ISO в хранилище данных PRIVATE-C9P42W2.A.INTERNAL самой виртуальной машины (VM) контроллера, поскольку общедоступное хранилище данных недоступно. Во-вторых, загрузите файл `reset.iso` на узлы A и B виртуальной машины контроллера и примените его на этих узлах. Это действие гарантирует, что после возврата системы в нормальный режим и появления возможности доступа в PowerStore Manager будет отображаться запрос на ввод нового пароля как для пользователей-администраторов, так и для сервисных пользователей.

Действия

1. В vSphere в разделе **Storage** выберите свое устройство PowerStore X model.

   Например, **DataCenter-WX-D6013** > **PowerStore D6013**

2. В разделе **Files** выберите **ISOs**.
3. Выберите **Upload** и загрузите файл `reset.iso`: предварительно созданный файл образа из www.dell.com/support или свой собственный файл образа, созданный в системе Linux.
   Файл `reset.iso` появится в папке **ISOs**.
4. В vSphere в разделе **Host and Clusters** выберите первичный узел главного устройства PowerStore X model в кластере.

   Например, **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. В разделе **Summary** нажмите **CD/DVD drive 1** и выберите **Connect to datastore ISO file**.
   Откроется окно **Choose an ISO image to mount**.
6. В разделе **Datastores** нажмите главное устройство PowerStore X model в кластере и выберите папку **ISOs**.
   Файл `reset.iso` должен отобразиться в разделе **Contents**.
7. Выберите файл `reset.iso` и нажмите **OK**.
   В разделе **Summary** для **CD/DVD drive 1** около 10 секунд должно отображаться значение **Connected**, а затем поменяться на **Disconnected**. Пароль администратора кластера и (или) сервисный пароль будут сброшены к значениям по умолчанию.
8. Подключитесь к кластеру с помощью браузера, используя IP-адрес кластера, и войдите в качестве администратора с первоначальным паролем по умолчанию — **`Password123#`**.
   Отобразится запрос на сброс пароля администратора, пароля сервисной учетной записи или обоих паролей. Чтобы сбросить пароль сервисной учетной записи с помощью протокола SSH, используйте первоначальное значение пароля сервисной учетной записи по умолчанию — **`service`**.
9. Измените значение пароля администратора по умолчанию на пользовательское.
10. Чтобы пароль сервисной учетной записи отличался от пароля администратора, снимите соответствующий флажок.

Результат

Если после выполнения этой процедуры запрос на сброс пароля так и не отобразится при попытке входа в систему, обратитесь к поставщику услуг.

Сертификаты

Данные в хранилище сертификатов PowerStore хранятся постоянно. В хранилище сертификатов хранятся сертификаты следующих типов:

- сертификаты источника сертификатов (CA);
- сертификаты клиентов;
- сертификаты серверов.

Просмотр сертификатов

Об этой задаче

Для каждого сертификата, хранящегося в устройстве, в PowerStore Manager отображается следующая информация:

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

ПРИМЕЧАНИЕ: Для просмотра дополнительной информации о сертификатах используйте программный интерфейс REST API или интерфейс командной строки.

Чтобы просмотреть сведения о сертификате, выполните следующие действия:

Действия

1. Запустите PowerStore Manager.
2. Щелкните **Settings** и в разделе **Security** щелкните **Certificates**.
   Отобразятся сведения о сертификатах, хранящихся на устройстве.
3. Чтобы просмотреть цепочку сертификатов, включающую сертификат, и связанную с этим информацию для некоторого сервиса, нажмите этот сервис.
   Отобразится окно **View Certificate Chain** с информацией о цепочке сертификатов, включающей сертификат.

Безопасное соединение между устройствами PowerStore в кластере

При создании кластера первичный узел главного устройства кластера создает сертификат источника сертификатов (CA), также называемого источником сертификатов кластера. Главное устройство передает сертификат источника сертификатов кластера устройствам, присоединяющимся к кластеру.

Каждое устройство PowerStore в кластере создает собственный уникальный сертификат IPsec, который подписывается сертификатом источника сертификатов кластера. Для защиты конфиденциальных данных, которые устройства PowerStore передают по своей сети кластера, используются протоколы IPsec и TLS, благодаря чему обеспечиваются безопасность и целостность данных.

Безопасное соединение для репликации и импорта данных

Предусмотренная в PowerStore инфраструктура сертификатов и учетных данных позволяет осуществлять обмен сертификатами сервера и клиентов, а также учетными данными пользователей. Этот процесс включает следующие операции:

- извлечение и проверку сертификата сервера при подтверждении подключения TLS;
- добавление сертификата доверенного ЦС из удаленной системы в хранилище учетных данных;
- добавление сертификата доверенного сервера/клиента в хранилище учетных данных;
- помощь в установлении безопасных соединений после установления доверия.

PowerStore поддерживает следующие функции управления сертификатами:

- Обмен сертификатами между двумя кластерами PowerStore для установления доверенного соединения управления при проведении репликации. Для осуществления репликации между кластерами PowerStore необходимо установить двустороннее доверие между кластерами, чтобы обеспечить взаимную аутентификацию по протоколу TLS при создании запросов на управление REST репликации.
- Обмен сертификатами и учетными данными с обеспечением сохраняемости для установления безопасного соединения между системой хранения Dell EMC (VNX, Unity, Storage Center (SC) или одноранговой системой хранения (PS)) и кластером PowerStore при проведении импорта данных.

Поддержка vSphere Storage API for Storage Awareness

vSphere Storage API for Storage Awareness (VASA) — это определенный в VMware независимый от поставщика программный интерфейс (API) для обнаружения СХД. VASA Provider включает в себя несколько компонентов, которые совместно работают для обслуживания поступающих API-запросов VASA. Шлюз API VASA, который получает все поступающие запросы API VASA, разворачивается на главном устройстве (которое владеет плавающим IP-адресом) в кластере PowerStore. Хосты ESXi и сервер vCenter Server подключаются к VASA Provider и получают информацию о доступной топологии хранилища, его возможностях и состоянии. После чего сервер vCenter предоставляет эту информацию клиентам vSphere. VASA используется клиентами VMware, а не клиентами PowerStore Manager.

Пользователь vSphere должен настроить экземпляр VASA Provider в качестве поставщика информации VASA для кластера. В случае отключения ведущего устройства связанный с ним процесс и VASA Provider перезапустятся на следующем главном устройстве. Аварийное переключение IP-адреса происходит автоматически. Внутри системы протокол обнаружит ошибку, когда получит события изменения конфигурации от нового активного экземпляра VASA Provider. Но это вызовет автоматическую повторную синхронизацию объектов VASA без участия пользователя.

PowerStore предоставляет интерфейсы VASA 3.0 для vSphere 6.5 и 6.7.

VASA 3.0 поддерживает Virtual Volumes (vVols). VASA 3.0 поддерживает интерфейсы для отправки запросов в абстракции хранилищ, такие как vVols и контейнеры хранилища. Эти сведения помогают системе управления хранилищем на основе политик (SPBM) принимать решения относительно размещения виртуальных дисков и комплаенса. VASA 3.0 также поддерживает интерфейсы для предоставления ресурсов и управления жизненными циклами vVols, которые используются для резервного копирования виртуальных дисков. Эти интерфейсы вызываются непосредственно хостами ESXi.

Для получения дополнительной информации, связанной с VASA, vSphere и vVols см. документацию VMware и онлайн-справку PowerStore Manager.

Аутентификация для VASA

Чтобы инициировать подключение vCenter к VASA Provider PowerStore Manager, введите в клиенте vSphere следующую информацию:

- URL-адрес VASA Provider, используя следующий формат для VASA 3.0: https://<IP-адрес управления>:8443/version.xml.
- Имя пользователя PowerStore Manager (обязательно с ролью администратора или администратора ВМ).

  ПРИМЕЧАНИЕ: Роль администратора виртуальной машины используется исключительно для регистрации сертификатов.
- Пароль, связанный с этим пользователем.

Учетные данные PowerStore Manager используются только на этом первоначальном этапе подключения. Если учетные данные PowerStore Manager действуют в целевом кластере, сертификат сервера vCenter автоматически регистрируется в кластере. Этот сертификат будет использоваться для аутентификации всех последующих запросов от vCenter. Для установки или загрузки этого сертификата в VASA Provider никаких действий выполнять вручную не требуется. Если сертификат просрочен, vCenter должен зарегистрировать новый сертификат для обеспечения новой сессии. Если сертификат отозван пользователем, сессия становится недействительной, а подключение разрывается.

Сессия vCenter, безопасное подключение и учетные данные

Сессия vCenter начинается, когда администратор vSphere с помощью клиента vSphere передает серверу vCenter Server URL-адрес и учетные данные входа VASA Provider. Сервер vCenter Server использует URL-адрес, учетные данные и SSL-

сертификат VASA Provider для установления безопасного соединения с VASA Provider. Сессия vCenter завершается, когда происходит одно из следующих событий:

- Администратор использует клиент vSphere для удаления VASA Provider из конфигурации vCenter, и сервер vCenter Server разрывает соединение.
- В работе сервера vCenter происходит сбой, или происходит сбой сервиса сервера vCenter, в результате чего подключение разрывается. Если vCenter или сервису сервера vCenter не удается восстановить SSL-подключение, устанавливается новое подключение.
- Происходит сбой VASA Provider, что приводит к прерыванию подключения. При перезапуске VASA Provider может отреагировать на запросы связи со стороны vCenter Server, чтобы восстановить SSL-подключение и прерванную сессию VASA.

В сессии vCenter используется безопасный обмен данными по протоколу HTTPS между сервером vCenter Server и VASA Provider. При использовании VASA 3.0 сервер vCenter выполняет роль источника сертификатов VMware (VMCA). VASA Provider передает самоподписанный сертификат при получении запроса, предварительно авторизовав запрос. Он добавляет сертификат VMCA в свое хранилище доверенных сертификатов, а затем отправляет запрос на подпись сертификата и заменяет свой самоподписанный сертификат сертификатом, подписанным VMCA. Для аутентификации последующих подключений VASA Provider будет использовать сертификат службы мониторинга хранилища (SMS) клиента, проверяемый по ранее зарегистрированному корневому сертификату подписи. VASA Provider создает уникальные идентификаторы для объектов в хранилище, а сервер vCenter Server использует их для запроса данных по конкретным объектам.

VASA Provider использует сертификаты SSL и идентификатор сессии VASA для валидации сессий VASA. После установления сессии VASA Provider должен проверить сертификат SSL и идентификатор сессии VASA, связанные с каждым вызовом функции с сервера vCenter Server. VASA Provider использует сертификат VMCA, хранящийся в его хранилище доверенных сертификатов, для валидации сертификата, связанного с вызовами функций из vCenter SMS. Сессия VASA сохраняется между несколькими SSL-подключениями. Если соединение по протоколу SSL прервется, сервер vCenter Server выполнит процедуру подтверждения подключения по протоколу SSL при участии VASA Provider, чтобы восстановить соединение по протоколу SSL в контексте той же сессии VASA. Если срок действия сертификата SSL истекает, администратор vSphere должен создать новый сертификат. Сервер vCenter Server установит новое соединение по протоколу SSL и зарегистрирует новый сертификат с VASA Provider.

ОСТОРОЖНО: Сервис SMS не вызывает функцию `unregisterVASACertificate` в отношении 3.0 VASA Provider. Таким образом, даже после отмены регистрации VASA Provider может продолжать использовать свой полученный от SMS сертификат, подписанный VMCA.

Аутентификация CHAP

Протокол аутентификации с косвенным согласованием (CHAP) — это метод аутентификации инициаторов iSCSI (хостов) и целевых ресурсов (томов и моментальных снимков). CHAP обеспечивает доступ к хранилищу iSCSI и выступает в роли безопасного стандартного протокола хранения. Аутентификация зависит от секрета, аналогичного паролю и известного как аутентификатору, так и одноранговому узлу. Существует два варианта протокола CHAP:

- Односторонняя аутентификация CHAP позволяет целевому ресурсу iSCSI аутентифицировать инициатор. Когда инициатор пытается подключиться к целевому устройству (в обычном режиме или в режиме обнаружения), он предоставляет целевому устройству имя пользователя и пароль.
- В дополнение к односторонней аутентификации CHAP применяется взаимная аутентификация. Взаимная аутентификация CHAP позволяет целевому ресурсу iSCSI и инициатору аутентифицировать друг друга. Каждый целевой ресурс iSCSI, представленный в группе, аутентифицируется инициатором iSCSI. Когда инициатор пытается подключиться к целевому ресурсу, целевой ресурс предоставляет инициатору имя пользователя и пароль. Инициатор сравнивает предоставленные имя пользователя и пароль с хранящейся в нем информацией. Если они совпадают, инициатор может подключиться к целевому ресурсу.

ПРИМЕЧАНИЕ: Если протокол CHAP будет использоваться в вашей среде, рекомендуется настроить и включить аутентификацию CHAP до того, как будет выполняться подготовка томов к получению данных. Если вы подготовите накопители к получению данных до настройки и включения аутентификации CHAP, доступ к томам может быть потерян.

PowerStore не поддерживает режим обнаружения по протоколу CHAP для iSCSI. В приведенной ниже таблице показаны ограничения PowerStore, связанные с режимом обнаружения по протоколу CHAP для iSCSI.

Таблица 1. Ограничения режима обнаружения по протоколу CHAP для iSCSI

Режим CHAP	Односторонний режим (активирован инициатор)	Взаимный режим (активированы инициатор и целевое устройство)
Обнаружение	PowerStore не будет аутентифицировать (проверять) хост. Аутентификацию невозможно использовать для предотвращения обнаружения целевых устройств. Это не приводит к непредусмотренному доступу к пользовательским данным.	PowerStore не будет отвечать на запрос аутентификации (проверки подлинности) от хоста, и обнаружение завершится сбоем, если хост предпримет проверку подлинности PowerStore.
Обычный	Работает должным образом. PowerStore проверяет учетные данные.	Работает должным образом. PowerStore передает учетные данные.

Во время удаленной репликации между исходным и целевым устройствами процесс проверки и обновления обнаруживает изменения в локальной и удаленной системах и повторно устанавливает подключения для обмена данными, учитывая при этом действующие настройки CHAP.

Настройка CHAP

Для кластера PowerStore можно активировать одностороннюю (активирован инициатор) или взаимную (инициатор и целевое устройство) аутентификацию по протоколу CHAP. Аутентификацию CHAP можно включить для кластера с одним или несколькими устройствами PowerStore и внешними хостами.

Если включена односторонняя аутентификация, потребуется ввести имя пользователя и пароль для каждого инициатора при добавлении внешних хостов. Если включена взаимная аутентификация, также потребуется ввести имя пользователя и пароль для кластера. При добавлении хоста и инициаторов с включенным протоколом CHAP пароль инициатора должен быть уникальным. Нельзя использовать одинаковые пароли для нескольких инициаторов хоста. Подробные указания по настройке конфигурации CHAP на внешнем хосте могут варьироваться. Чтобы использовать эту возможность, следует ознакомиться с операционной системой хоста и способом ее настройки.

ПРИМЕЧАНИЕ: Включение CHAP после настройки хостов в системе приводит к нарушениям в работе внешних хостов. Это прерывает операции ввода-вывода до тех пор, пока настройки не будут заданы на внешнем хосте и на устройстве. Перед добавлением внешних хостов на устройство рекомендуется решить, какой тип конфигурации CHAP планируется реализовать (если использование этого протокола вообще запланировано).

Если вы включили CHAP после добавления хостов, обновите инициаторы на каждом хосте. Если CHAP включен, нельзя добавить хост в группу хостов, у которой нет учетных данных CHAP. После включения CHAP и последующего добавления хоста вручную зарегистрируйте хост в PowerStore Manager, для чего в разделе **Compute** выберите **Hosts & Host Groups**. Вам потребуется ввести учетные данные на уровне iSCSI для целей аутентификации. В этом случае скопируйте IQN с хоста, а затем добавьте связанные учетные данные CHAP для каждого инициатора.

Настройте протокол CHAP для кластера с помощью любого из следующих средств:

- **CHAP** — страница параметров CHAP, доступ к которой возможен из PowerStore Manager (нажмите **Settings** и в разделе **Security** выберите **CHAP**).
- Сервер REST API — прикладной интерфейс, который может принимать запросы REST API для настройки параметров CHAP. Дополнительные сведения о REST API см. в документе *PowerStore REST API Reference Guide*.

Чтобы определить состояние протокола CHAP, в PowerStore Manager нажмите **Settings** и в разделе **Security** выберите **CHAP**.

Внешний доступ по протоколу SSH

На каждом устройстве можно дополнительно включить доступ посредством внешнего протокола безопасной оболочки (SSH) к порту SSH IP-адреса устройства, чтобы пользователь мог воспользоваться функцией обслуживания на первичном узле устройства. IP-адрес устройства перемещается между двумя узлами устройства по мере изменения главного места назначения. Если внешний доступ по протоколу SSH отключен, доступ по протоколу SSH разрешаться не будет.

Изначально в устройстве (до его настройки) протокол SSH активирован по умолчанию, чтобы устройство можно было обслужить, если в нем возникнут проблемы до его добавления в кластер. При создании нового кластера или выполнении операции присоединения к кластеру протокол SSH должен быть отключен на всех устройствах.

Настройка внешнего доступа по протоколу SSH

Внешний доступ по протоколу SSH к устройствам в кластере можно настроить с помощью любого из следующих средств:

- **SSH Management** — страница настройки параметров SSH, доступ к которой возможен из PowerStore Manager (нажмите **Settings** и в разделе **Security** выберите **SSH Management**).
- Сервер REST API — прикладной интерфейс, который может принимать запросы REST API для настройки параметров SSH. Дополнительные сведения о REST API см. в документе *PowerStore REST API Reference Guide*.
- `svc_service_config` — сервисная команда, которую можно непосредственно ввести на устройстве в качестве сервисного пользователя. Дополнительную информацию об этой команде см. в документе *PowerStore Service Scripts Guide*.

Чтобы определить состояние SSH на устройствах в пределах кластера, в PowerStore Manager нажмите **Settings** и в разделе **Security** выберите **SSH Management**. Вы также можете активировать или отключить SSH на одном или нескольких устройствах по вашему выбору.

После успешного включения сервиса SSH перейдите на IP-адрес устройства с помощью любого клиента SSH. Для доступа к устройству необходимо указать учетные данные пользователя сервисного обслуживания.

Сервисная учетная запись дает возможность пользователям выполнять следующие функции:

- Выполнение специальных сервисных скриптов для устройства с целью мониторинга, а также поиска и устранения неполадок, связанных с параметрами и функционированием системы устройства.
- Использование лишь ограниченного набора команд, которые назначаются члену непривилегированной учетной записи пользователя Linux в режиме ограниченной оболочки. Данная учетная запись не позволяет получить доступ к проприетарным системным файлам, файлам конфигурации либо данным пользователей или заказчиков.

В целях обеспечения максимальной безопасности устройства рекомендуется, чтобы внешний сервисный интерфейс SSH был все время выключен, кроме случаев, когда он действительно нужен для выполнения сервисных операций для устройства. После выполнения необходимых сервисных операций интерфейс SSH следует сразу же отключать для обеспечения безопасности устройства.

Сессии SSH

Сессии сервисного интерфейса SSH PowerStore осуществляются в соответствии с параметрами, установленными клиентом SSH. Характеристики сессий зависят от параметров конфигурации клиента SSH.

Пароль сервисной учетной записи

Сервисная учетная запись — это учетная запись, с помощью которой персонал службы технической поддержки может выполнять базовые команды Linux.

Во время начальной настройки устройства необходимо изменить сервисный пароль по умолчанию. Для сервисного пароля применяются те же ограничения, что и для учетных записей управления системой (см. раздел Использование имени пользователя и пароля на стр. 7).

Авторизация по протоколу SSH

Авторизация сервисных учетных записей основана на следующем:

- Изоляция приложений — программное обеспечение PowerStore использует технологию контейнеров, которая обеспечивает изоляцию приложений. Доступ к устройству для сервисных целей обеспечивается сервисным контейнером. Предоставляется только набор сервисных скриптов и набор команд Linux. У сервисной учетной записи нет возможности получить доступ к другим контейнерам, которые обслуживают пользовательские операции ввода-вывода файловой системы и блочного ввода-вывода.
- Разрешения файловой системы Linux — большинство инструментов и утилит Linux, которые тем или иным образом изменяют работу системы, недоступны для сервисного пользователя и требуют прав учетной записи суперпользователя. Так как у сервисной учетной записи нет таких прав доступа, она не позволяет использовать средства и служебные программы Linux, для которых отсутствует разрешение на выполнение, и не позволяет изменять файлы конфигурации, требующие доступа с правами root для чтение и/или изменения.
- Контроль доступа — помимо изоляции приложений, обеспечиваемой контейнерной технологией, механизм списка контроля доступа (ACL) в устройстве использует список очень точно сформулированных правил для явного

предоставления доступа к системным ресурсам для сервисной учетной записи или отказа в доступе к этим ресурсам. Эти правила определяют разрешения сервисной учетной записи для других компонентов устройства, которые не определены другим образом стандартными разрешениями для файловой системы Linux.

Сервисные скрипты устройства

Версия программного обеспечения устройства включает набор скриптов для диагностики проблем, настройки системы и ее восстановления. Эти скрипты позволяют получать всестороннюю информацию и дают возможность управлять системой на более низком уровне, чем это возможно с PowerStore Manager. Эти скрипты и типичные сценарии их использования описываются в документе *PowerStore Service Scripts Guide*.

Сервисный порт Ethernet узла устройства и IPMItool

Устройство предоставляет доступ к консоли через сервисный порт Ethernet, имеющийся на каждом узле. Для этот требуется программа IPMItool. IPMItool — это сетевое средство, аналогичное SSH или Telnet, которое взаимодействует с каждым узлом через Ethernet-соединение с использованием протокола IPMI. IPMItool — это утилита Windows, которая создает защищенный канал связи для доступа к консоли узла устройства. Для активации консоли этой утилите требуется физический доступ.

Интерфейс сервисного порта Ethernet узла поддерживает те же функции, что и сервисный интерфейс SSH (сервисный интерфейс локальной сети), и к нему применяются те же ограничения. Однако пользователи получают доступ к интерфейсу по соединению с портом Ethernet, а не через клиент SSH. Этот интерфейс предназначен для того, чтобы специалисты службы поддержки при обслуживании системы на месте могли подключиться к устройству без вмешательства в сеть. Выделенная консоль управления не требуется.

Этот интерфейс обеспечивает прямое подключение «от точки к точке» без маршрутизации. Специалисты службы поддержки могут использовать сервисный интерфейс локальной сети для вывода данных на консоль, а также для доступа по протоколу SSH к сервисному контейнеру PowerStore и PowerStore Manager, включая мастер начальной настройки (ICW). Доступ по протоколу SSH к сервисному контейнеру через сервисный интерфейс локальной сети всегда активирован и не может быть отключен; однако учетными данными сервисной учетной записи управляете вы.

Список сервисных скриптов см. в документе *PowerStore Service Scripts Guide*.

Безопасность NFS

Под безопасностью NFS подразумевается использование протокола Kerberos для аутентификации пользователей в сетевых файловых системах NFSv3 и NFSv4. Протокол Kerberos обеспечивает целостность (использование подписей) и конфиденциальность (шифрование) данных. Однако обеспечение целостности и конфиденциальности активировать необязательно — эти функции являются необязательными параметрами экспорта NFS.

В отсутствие Kerberos сервер возлагает функции аутентификации пользователей исключительно на клиента и доверяет клиенту. Если же используется протокол Kerberos, сервер доверяет центру распределения ключей (KDC). В этом случае именно центр распределения ключей отвечает за аутентификацию и управляет учетными записями (участниками) и паролями. Более того, никакие пароли не передаются по сети в какой бы то ни было форме.

Без использования Kerberos учетные данные пользователя передаются по сети в незашифрованном виде, и поэтому их можно легко подделать. При использовании Kerberos удостоверение (субъект) пользователя включается в зашифрованный билет Kerberos, который может быть прочитан только целевым сервером и KDC. Только им одним известен ключ шифрования.

В сочетании с безопасностью NFS поддерживаются алгоритмы шифрования AES128 и AES256 в Kerberos. Помимо собственно безопасности NFS это также затрагивает протоколы SMB и LDAP. Теперь эти алгоритмы шифрования по умолчанию поддерживаются в Windows и Linux. Эти алгоритмы обеспечивают намного более высокий уровень защиты, однако они могут и не использоваться — это зависит от клиента. На основании данных участника-пользователя сервер создает учетные данные этого пользователя, запрашивая активную службу UDS (Unix Directory Service). Поскольку система NIS не является защищенной, ее не рекомендуется использовать совместно с безопасностью NFS. Рекомендуется использовать Kerberos с протоколом LDAP или LDAPS.

Безопасность NFS можно настроить с помощью PowerStore Manager.

Взаимосвязи файловых протоколов

При использовании Kerberos потребуется следующее:

- DNS — вместо IP-адресов следует использовать DNS-имя.
- NTP — PowerStore должен иметь настроенный сервер NTP.

  ПРИМЕЧАНИЕ: Kerberos использует правильную синхронизацию времени между KDC, серверами и клиентом в сети.
- UDS — для создания учетных данных.
- Имя хоста — Kerberos работает с именами, а не с IP-адресами.

Безопасность NFS использует одно или два имени субъектов-служб (SPN) в зависимости от значения имени хоста. Если имя хоста имеет формат полного доменного имени — хост.домен:

- короткое имя SPN: **`nfs/host@REALM`**;
- длинное имя SPN: **`nfs/host.domainFQDN@REALM`**.

Если имя хоста не представлено в формате полностью определенного доменного имени, используется только короткое имя SPN.

Аналогично системе SMB, где сервер SMB можно присоединить к домену, сервер NFS можно присоединить к области (эквивалент домена в терминологии Kerberos). Это можно сделать одним из двух указанных ниже способов.

- Использовать настроенный домен Windows (при его наличии).
- Полностью настроить область Kerberos на основе KDC UNIX.

Если администратор решает использовать настроенный домен Windows, больше ничего настраивать не требуется. Каждое имя SPN, используемое сервисом NFS, автоматически добавляется в KDC или удаляется из него при присоединении или отсоединении сервера SMB. Следует отметить, что, если для безопасности NFS настроено использование конфигурации SMB, сервер SMB не может быть уничтожен.

Если администратор решает использовать область Kerberos на основе UNIX, дополнительно требуется:

- Имя области: имя области Kerberos, которая обычно содержит только буквы в верхнем регистре.
- полностью настроить область Kerberos на основе KDC UNIX.

Для того чтобы клиент подключал экспорт NFS с конкретным значением уровня безопасности, предусмотрен параметр безопасности sec, который указывает минимально допустимый уровень безопасности. Существует четыре механизма обеспечения безопасности:

- `AUTH_SYS`: стандартный устаревший механизм обеспечения безопасности, который не использует Kerberos. Сервер доверяет учетным данным, которые предоставляются клиентом.
- `KRB5`: аутентификация с использованием Kerberos v5.
- `KRB5i`: аутентификация средствами Kerberos в сочетании с обеспечением целостности (использованием подписей).
- `KRB5p`: аутентификация средствами Kerberos в сочетании с обеспечением целостности и конфиденциальности (шифрованием).

Если клиент NFS пытается подключить экспортированный объект, уровень безопасности которого ниже установленного минимума, доступ будет запрещен. Например, если в качестве минимального параметра для доступа установлен `KRB5i`, любые подключаемые объекты, использующие `AUTH_SYS` или `KRB5`, будут отклонены.

Создание учетных данных

При подключении пользователя к системе он представляет только свой субъект (**`user@REALM`**), который извлекается из билета Kerberos. В отличие от механизма обеспечения безопасности `AUTH_SYS`, в этом случае учетные данные не включаются в запрос NFS. Часть, обозначающая пользователя (перед символом @), извлекается из субъекта и используется для поиска соответствующего идентификатора UID в UDS. Система создает учетные данные на основании найденного UID, используя активную службу UDS, — точно так же, как в случае, когда активированы расширенные учетные данные NFS (с тем лишь исключением, что в отсутствие Kerberos идентификатор UID предоставляется непосредственно по запросу).

Если участник в службе UDS не сопоставлен, используются настроенные учетные данные пользователя UNIX по умолчанию. Если пользователь UNIX по умолчанию не настроен, используются учетные данные пользователя nobody.

Безопасность объектов файловой системы

В среде с несколькими протоколами политика безопасности настраивается на уровне файловой системы отдельно для каждой файловой системы. Каждая файловая система на основании настроенной для нее политики безопасности определяет способ урегулирования различий в семантике контроля доступа протоколов NFS и SMB. Выбранная политика доступа определяет, какой механизм применяется для обеспечения безопасности файлов в конкретной файловой системе.

ПРИМЕЧАНИЕ: Если в вашей инфраструктуре должен поддерживаться более старый протокол SMB1, его можно активировать с помощью сервисной команды `svc_nas_cifssupport`. Дополнительную информацию об этой сервисной команде см. в документе *PowerStore Service Scripts Guide*.

Модель безопасности UNIX

Если выбрана политика UNIX, любые попытки изменить параметры безопасности на уровне файлов по протоколу SMB, например внести изменения в списки контроля доступа, игнорируются. Права доступа UNIX задаются битами режимов или списком контроля доступа NFSv4 объекта файловой системы. Биты режимов представлены битовой строкой. Каждый бит указывает режим доступа или полномочия, которые предоставлены пользователю, владеющему файлом; группе, связанной с объектом файловой системы; и всем остальным пользователям. Биты режимов UNIX представлены в виде трех наборов объединенных триплетов rwx (чтение, запись и выполнение) для каждой категории пользователей (пользователь, группа и прочие). Список контроля доступа (ACL) — это список пользователей и групп пользователей, на основании которого пользователям предоставляется доступ к сервисам или, наоборот, отказывается в доступе.

Модель безопасности Windows

Модель безопасности Windows построена главным образом на назначении прав для объектов с использованием дескриптора безопасности (SD) и его списка контроля доступа (ACL). Если выбрана политика SMB, изменения битов режимов по протоколу NFS игнорируются.

Доступ к объекту файловой системы основан на том, задано ли для разрешений значение «Разрешить» или «Запретить» с помощью дескриптора безопасности. Дескриптор безопасности (SD) задает владельца объекта и идентификаторы SID групп для объекта вместе со списками ACL. Список ACL является частью дескриптора безопасности для каждого объекта. Каждый список ACL содержит записи контроля доступа (ACE). В свою очередь, каждый список ACE содержит один идентификатор SID, который идентифицирует пользователя, группу или компьютер, а также список прав, запрещенных или разрешенных для этого идентификатора SID.

Доступ к файловым системам в среде с несколькими протоколами

Доступ к файлам обеспечивается через серверы NAS. Сервер NAS содержит набор файловых систем, в которых хранятся данные. Сервер NAS предоставляет доступ к этим данным файловым протоколам NFS и SMB путем совместного использования файловых систем с помощью общих ресурсов SMB и NFS. Режим сервера NAS для многопротокольного общего доступа обеспечивает общий доступ к одним и тем же данным с помощью протоколов SMB и NFS. Поскольку режим многопротокольного общего доступа обеспечивает одновременный доступ к файловой системе по протоколам SMB и NFS, необходимо правильно учесть и настроить сопоставление пользователей Windows с пользователями Unix, а также определить используемые правила безопасности (биты режимов, список управления доступом и учетные данные пользователей) для многопротокольного общего доступа.

ПРИМЕЧАНИЕ: Информацию о настройке серверов NAS и управлении ими в отношении многопротокольного общего доступа, сопоставления пользователей, политик доступа и учетных данных пользователей см. в онлайн-справке PowerStore Manager.

Сопоставление пользователей

В многопротокольном контексте пользователь Windows должен сопоставляться с пользователем UNIX. Однако пользователь UNIX должен сопоставляться с пользователем Windows только в том случае, если используется политика доступа Windows. Установка соответствия между пользователями необходима для того, чтобы средства безопасности

файловой системы могли принудительно применяться, даже если они не встроены в тот или иной протокол. В сопоставлении пользователей участвуют следующие компоненты:

- службы каталогов UNIX и/или локальные файлы;
- Сопоставители Windows
- безопасная установка соответствия (secmap) — кэш-память, содержащая все соответствия между идентификаторами SID и UID или GID, используемыми сервером сетевой системы хранения данных;
- ntxmap.

ПРИМЕЧАНИЕ: Сопоставление пользователей не влияет на пользователей и группы, которые являются локальными для сервера SMB.

Службы каталогов UNIX и локальные файлы

Службы каталогов UNIX (UDS) и локальные файлы используются для выполнения следующих действий:

- возвращают имя соответствующей учетной записи UNIX для определенного идентификатора пользователя (UID);
- возвращают соответствующий идентификатор UID и главный идентификатор GID для имени определенной учетной записи UINIX.

Поддерживаются следующие службы:

- LDAP
- NIS
- Локальные файлы
- Нет (установка соответствия возможна только через пользователя по умолчанию)

В том случае если активирован многопротокольный общий доступ, для сервера сетевой системы хранения данных должна быть активирована одна служба каталогов UNIX (UDS) и/или локальные файлы. Что из этого будет использоваться для установки соответствия между пользователями, определяется свойством службы каталогов Unix сервера сетевой системы хранения данных.

Сопоставители Windows

Сопоставители Windows используются для выполнения следующих действий при сопоставлении пользователей:

- возвращают имя соответствующей учетной записи Windows для определенного идентификатора безопасности (SID);
- возвращают соответствующий идентификатор безопасности (SID) для определенного имени учетной записи Windows.

Сопоставителями Windows могут быть:

- контроллер домена (DC);
- база данных локальных групп (LGDB) сервера SMB.

secmap

Безопасная установка соответствия (secmap) служит для хранения всех соответствий между идентификаторами SID и UID/главным идентификатором GID и между идентификаторами UID и SID, обеспечивая согласованность во всех файловых системах сервера сетевой системы хранения данных.

ntxmap.

ntxmap служит для связывания учетной записи Windows с учетной записью UNIX, если их имена различаются. Например, если учетная запись пользователя в Windows имеет имя Gerald, а учетная запись в UNIX имеет имя Gerry, связь между двумя этими учетными записями устанавливается файлом ntxmap.

Сопоставление идентификаторов SID и UID, сопоставления главного идентификатора GID

Ниже описан порядок определения идентификатора UID/главного идентификатора GID, соответствующих идентификатору SID.

1. Выполняется поиск идентификатора SID в secmap. Если SID найден, определяются соответствующие ему идентификаторы UID и GID.
2. Если SID в secmap не найден, необходимо найти имя Windows, относящееся к SID.
   a. Выполняется поиск идентификатора SID в базе данных локальных групп серверов SMB сетевой системы хранения данных. Если SID найден, соответствующее ему имя Windows определяется как имя локального пользователя вместе с именем сервера SMB.
   b. Если идентификатор SID не найден в базе данных локальных групп, выполняется поиск контроллера домена. Если SID найден, соответствующее ему имя Windows является именем пользователя. Если идентификатор SID не удается сопоставить, доступ запрещается.
3. Имя Windows преобразуется в имя UNIX. Для этой цели используется файл ntxmap.
   a. Если в ntxmap найдено имя Windows, в качестве имени UNIX используется соответствующая запись.
   b. Если имя Windows в ntxmap не найдено, в качестве имени UNIX используется само имя Windows.
4. Производится поиск имени UNIX в службе каталогов Unix (UDS) (на сервере NIS, на сервере LDAP или в локальных файлах).
   a. Если имя пользователя UNIX найдено в UDS, определяются соответствующие ему идентификаторы UID и GID.
   b. Если имя UNIX не найдено, а функция автоматического сопоставление для несопоставленных учетных записей Windows включена, идентификатор UID назначается автоматически.
   c. Если имя пользователя UNIX в UDS не найдено, но есть учетная запись UNIX по умолчанию, идентификатор SID сопоставляется с идентификаторами UID и GID учетной записи UNIX по умолчанию.
   d. Если идентификатор SID не удается сопоставить, доступ запрещается.

Если соответствие найдено, оно добавляется в постоянную базу данных secmap. Если соответствие не найдено, в постоянную базу данных secmap добавляется запись о ненайденном соответствии.

На следующей диаграмме представлен порядок определения идентификатора UID и главного идентификатора GID, соответствующих идентификатору SID.

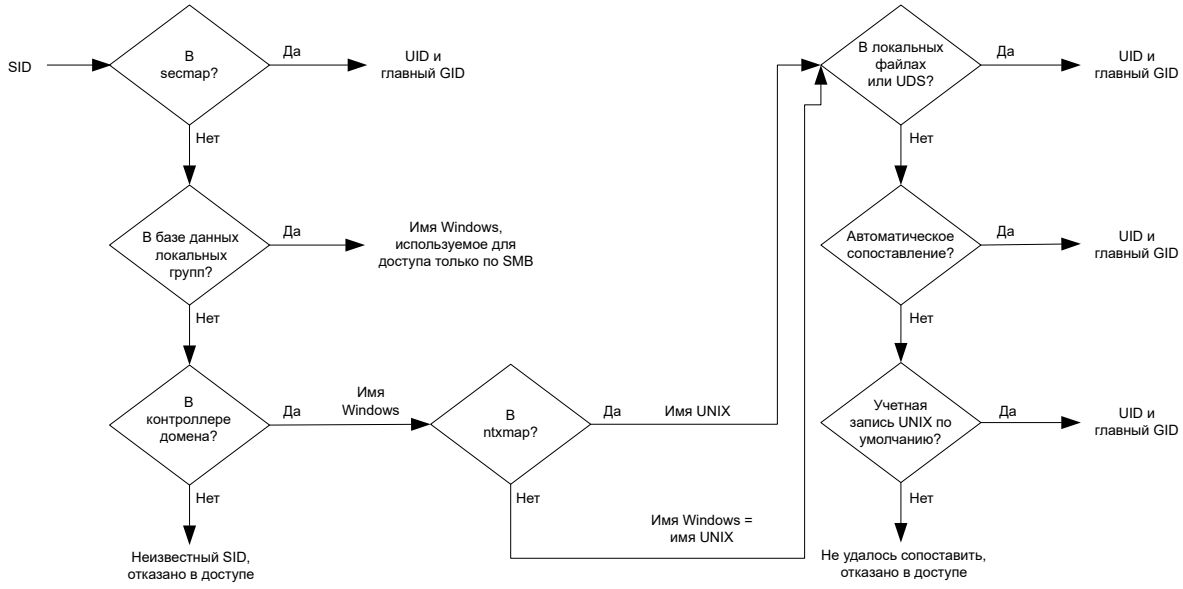

Рисунок 1. Процесс сопоставления идентификаторов SID и UID, сопоставления главного идентификатора GID

Установка соответствия между UID и SID

Ниже описан порядок определения идентификатора SID, соответствующего идентификатору UID.

1. Выполняется поиск идентификатора UID в secmap. Если UID найден, определяется соответствующий ему идентификатор SID.
2. Если UID в secmap не найден, необходимо найти имя UNIX, относящееся к UID.
   a. Производится поиск идентификатора UID в службе каталогов Unix (UDS) (на сервере NIS, на сервере LDAP или в локальных файлах). Если UID найден, соответствующее ему имя UNIX является именем пользователя.
   b. Если UID в UDS не найден, но есть учетная запись Windows по умолчанию, UID сопоставляется с SID учетной записи Windows по умолчанию.
3. Если данные учетной записи Windows по умолчанию не используются, имя UNIX преобразуется в имя Windows. Для этой цели используется файл ntxmap.
   a. Если в ntxmap найдено имя UNIX, в качестве имени Windows используется соответствующая запись.
   b. Если имя UNIX в ntxmap не найдено, в качестве имени UNIX используется имя Windows.
4. Выполняется поиск имени Windows в контроллере домена Windows или в базе данных локальных групп.
   a. Если имя Windows найдено, определяется соответствующий ему идентификатор SID.
   b. Если имя Windows содержит точку и часть имени после последней точки (.) совпадает с именем сервера SMB, выполняется поиск в базе данных локальных групп этого сервера SMB для сопоставления идентификатора SID.
   c. Если имя Windows не найдено, но имеется учетная запись Windows по умолчанию, идентификатор SID сопоставляется с этой учетной записью Windows по умолчанию.
   d. Если идентификатор SID не удается сопоставить, доступ запрещается.

Если соответствие найдено, оно добавляется в постоянную базу данных secmap. Если соответствие не найдено, в постоянную базу данных secmap добавляется запись о ненайденном соответствии.

На следующей диаграмме представлен порядок определения идентификатора SID, соответствующего идентификатору UID.

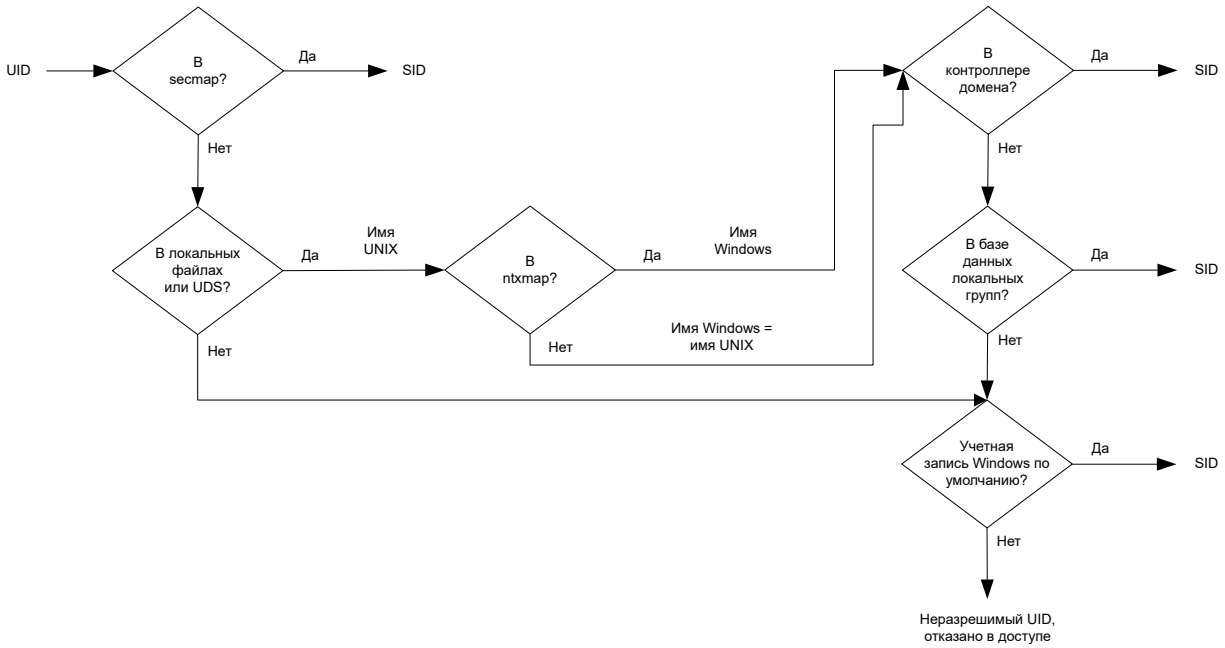

Рисунок 2. Порядок определения идентификатора SID, соответствующего идентификатору UID

Политики доступа для протоколов NFS, SMB и FTP

В среде с несколькими протоколами система хранения использует политики доступа файловой системы для управления доступом пользователей к файловым системам. Существует два вида безопасности: UNIX и Windows.

Для аутентификации в системе безопасности UNIX учетные данные создаются на основе служб каталогов UNIX (UDS), за исключением небезопасного доступа по протоколу NFS, при котором учетные данные предоставляются клиентом хоста. Права пользователей определяются на основе битов режимов и списка контроля доступа NFSv4. Для идентификации используется идентификаторы пользователей и групп (UID и GID, соответственно). С безопасностью UNIX не связаны никакие права.

В случае аутентификации на основе встроенных средств безопасности Windows учетные данные создаются с помощью контроллера домена (DC) Windows и базы данных локальных групп (LGDB) сервера SMB. Права пользователей определяются на основе списков контроля доступа (ACL) протокола SMB. Для идентификации используется идентификатор безопасности (SID). Существуют полномочия, связанные с безопасностью Windows (например, TakeOwnership, Backup и Restore), которые предоставляются базой данных LGDB или объектом групповой политики (GPO) сервера SMB.

В следующей таблице дается описание политик доступа, которые определяют, какой вид безопасности используется для каждого из протоколов:

Политика доступа	Описание
Собственная (по умолчанию)	• Каждый протокол управляет доступом с использованием своих собственных функций безопасности. • Для обеспечения безопасности сетевых папок NFS используются учетные данные UNIX, связанные с запросом на проверку битов режима UNIX NFSv3 или списка контроля доступа NFSv4. Затем доступ разрешается или запрещается. • Для обеспечения безопасности сетевых папок SMB используются учетные данные Windows, связанные с запросом на проверку списка контроля доступа SMB. Затем доступ разрешается или запрещается. • Биты режима UNIX NFSv3 и изменения разрешений ACL NFSv4 синхронизируются друг с другом. • Синхронизация между разрешениями Unix и Windows не выполняется.
Windows	• Доступ на уровне файлов для Windows и UNIX защищается с помощью системы безопасности Windows. • Для проверки ACL SMB используются учетные данные Windows. • Разрешения для только что созданных файлов определяются преобразованием ACL SMB. Изменения разрешений ACL SMB синхронизируются с ACL NFSv4 или битами режима UNIX NFSv3. • Биты режима NFSv3 и изменения разрешений ACL NFSv4 запрещаются.
UNIX	• Доступ на уровне файлов для Windows и UNIX защищается с помощью системы безопасности UNIX. • При запросе на доступ SMB для проверки битов режима NFSv3 или ACL NFSv4 в отношении разрешений используются учетные данные UNIX из локальных файлов или UDS. • Разрешения для только что созданных файлов определяются по UMASK. • Биты режима UNIX NFSv3 или изменения разрешений ACL NFSv4 синхронизируются с ACL SMB. • Изменения разрешений ACL SMB допустимы во избежание прерывания работы, но эти разрешения не сохраняются.

В случае протокола FTP аутентификация с помощью Windows или UNIX выбирается в зависимости от формата имени пользователя, который используется при аутентификации на сервере NAS. Если используется аутентификация Windows, контроль доступа по протоколу FTP аналогичен контролю доступа по протоколу SMB; в противном случае аутентификация аналогична аутентификации для файловой системы NFS. Аутентификация клиентов FTP и SFTP производится, когда они подключаются к серверу NAS. Это может быть аутентификация SMB (если имя пользователя указано в формате `domain\user` или `user@domain`) или аутентификация UNIX (для других форматов одиночного имени пользователя). Аутентификация SMB обеспечивается контроллером домена Windows, принадлежащим домену, который определен на сервере NAS. Аутентификация UNIX обеспечивается сервером NAS в соответствии с зашифрованным паролем, хранящимся на удаленном сервере LDAP, на удаленном сервере NIS или в локальном файле паролей сервера NAS.

Учетные данные для обеспечения безопасности на уровне файлов

Для обеспечения безопасности на уровне файлов система хранения должна создать учетные данные, связанные с обрабатываемым запросом протокола SMB или NFS. Существуют два вида учетных данных, Windows и UNIX. Учетные данные Windows и UNIX создаются сервером NAS для перечисленных ниже сценариев использования.

- Для создания учетных данных UNIX с более чем 16 группами для запроса NFS. Для того чтобы это было возможно, должно быть настроено свойство расширенных учетных данных сервера NAS.
- Для создания учетных данных UNIX для запроса SMB, когда для файловой системы выбрана политика доступа UNIX.
- Для создания учетных данных Windows для запроса SMB.
- Для создания учетных данных Windows для запроса NFS, когда для файловой системы выбрана политика доступа Windows.

ПРИМЕЧАНИЕ: Если свойство расширенных учетных данных не настроено, при обработке запроса NFS используются учетные данные UNIX, указанные в запросе NFS. Если для запроса SMB используется аутентификация на основе Kerberos, учетные данные Windows пользователя домена включаются в сертификат Kerberos запроса на установление сессии.

Постоянная кэш-память учетных данных используется:

- для учетных данных Windows, созданных для доступа к файловой системе, использующей политику доступа Windows;
- для учетных данных Unix, предназначенных для доступа по протоколу NFS, если расширенные учетные данные включены.

Для каждого сервера NAS имеется один экземпляр кэш-памяти.

Предоставление доступа несопоставленным пользователям

Для использования нескольких протоколов необходимо выполнение следующих требований:

- каждый пользователь Windows должен быть сопоставлен пользователю UNIX;
- пользователь UNIX должен быть сопоставлен пользователю Windows, чтобы можно было создать учетные данные Windows, когда этот пользователь обращается к файловой системе, в которой действует политика доступа Windows.

С сервером NAS связано два следующих свойства, относящихся к пользователям, для которых соответствие не установлено:

- пользователь UNIX по умолчанию;
- пользователь Windows по умолчанию.

Когда пользователь Windows, для которого не установлено соответствие, пытается подключиться к многопротокольной файловой системе, а для сервера NAS настроена учетная запись пользователя UNIX по умолчанию, в учетных данных Windows используются идентификатор пользователя (UID) и идентификатор главной группы (GID) пользователя UNIX по умолчанию. Аналогичным образом, когда несопоставленный пользователь UNIX пытается подключиться к многопротокольной файловой системе, а учетная запись пользователя Windows по умолчанию настроена для сервера NAS, используются учетные данные Windows пользователя Windows по умолчанию.

ПРИМЕЧАНИЕ: Если пользователь UNIX по умолчанию не задан в службе каталогов UNIX (UDS), несопоставленным пользователям в доступе по протоколу SMB отказывается. Если пользователь Windows по умолчанию не найден в контроллере домена Windows или в базе данных LGDB, несопоставленным пользователям отказывается в доступе по протоколу NFS к файловой системе, в которой применяется политика доступа Windows.

ПРИМЕЧАНИЕ: Пользователь UNIX по умолчанию может иметь допустимое имя существующей учетной записи UNIX или идентификатор в новом формате `@uid=`*`xxxx`*`,gid=`*`yyyy`*`@`, где *xxxx* и *yyyy* — это десятичные числовые значения идентификатора UID и главного идентификатора GID соответственно. Эти значения можно задать в системе с помощью PowerStore Manager.

Учетные данные UNIX для запросов NFS

Для обработки запросов NFS в файловой системе с несколькими протоколами или только с протоколом NFS, в которой применяется политика доступа UNIX или собственная политика доступа, должны использоваться учетные данные UNIX. Учетные данные UNIX всегда встраиваются в каждый запрос. Однако учетные данные ограничены 16 дополнительными

группами. Свойство `extendedUnixCredEnabled` сервера NFS обеспечивает возможность создания учетных данных, содержащих более 16 групп. Если это свойство задано, в активную службу UDS отправляется запрос с идентификатором UID для получения идентификатора GID главной группы и всех идентификаторов GID групп, к которым он принадлежит. Если идентификатор UID не найден в службе UDS, используются учетные данные UNIX, встроенные в запрос.

ПРИМЕЧАНИЕ: В случае безопасного доступа по протоколу NFS учетные данные всегда создаются с использованием UDS.

Учетные данные UNIX для запросов SMB

Для обработки запросов SMB в файловой системе с несколькими протоколами, в которой применяется политика доступа UNIX, во время установления сессии предварительно должны быть созданы учетные данные Windows для пользователя SMB. Идентификатор SID пользователя Windows используется для поиска имени из AD. Это имя затем используется (посредством ntxmap, если требуется) для поиска идентификаторов Unix (UID и GID) в UDS или в локальном файле (файле passwd). Принадлежащий пользователю идентификатор UID владельца включается в учетные данные Windows. При доступе к файловой системе с использованием политики доступа UNIX идентификатор UID пользователя используется для запроса службы UDS с целью создания учетных данных UNIX, аналогично созданию расширенных учетных данных для файловой системы NFS. Идентификатор UID требуется для управления квотами.

Учетные данные Windows для запросов SMB

Для обработки запросов SMB в файловой системе только с протоколом SMB или в многопротокольной файловой системе, где применяется политика доступа Windows или собственная политика доступа, должны использоваться учетные данные Windows. Учетные данные Windows для протокола SMB требуется создавать только один раз во время запроса установления сессии при подключении пользователя.

При использовании аутентификации Kerberos учетные данные пользователя включаются в сертификат Kerberos запроса установления сессии, в отличие от случая, когда используется NTLM (NT LAN Manager). Остальная информация запрашивается из контроллера домена Windows или LGDB. В случае Kerberos список идентификаторов SID дополнительных групп берется из сертификата Kerberos и из списка идентификаторов SID дополнительных локальных групп. Список прав берется из базы данных локальных групп. В случае с NTLM список идентификаторов SID дополнительных групп берется из контроллера домена (DC) Windows и из списка идентификаторов SID дополнительных локальных групп. Список прав берется из базы данных локальных групп.

Кроме того, из компонента установки соответствия между пользователями также извлекаются соответствующий идентификатор UID и главный идентификатор GID. Поскольку идентификатор SID главной группы не используется при проверке прав доступа, вместо него используется главный идентификатор GID UNIX.

ПРИМЕЧАНИЕ: NTLM — это более старый набор частных протоколов безопасности, который обеспечивает аутентификацию пользователей, а также целостность и конфиденциальность их данных. Kerberos — это открытый стандартный протокол, обеспечивающий более быструю аутентификацию за счет использования системы сертификатов. Kerberos обеспечивает более высокую безопасность для систем в сети, чем NTLM.

Учетные данные Windows для запросов NFS

Учетные данные Windows создаются или извлекаются только тогда, когда пользователь посредством запроса NFS обращается к файловой системе, в которой действует политика доступа Windows. Идентификатор UID извлекается из запроса NFS. Предусмотрена глобальная кэш-память учетных данных Windows с соответствующим временем хранения, которая помогает избежать создания учетных данных для каждого запроса NFS. Если учетные данные Windows найдены в этой кэш-памяти, никакие другие действия не требуются. Если учетные данные Windows не найдены, для поиска имени для UID запрашивается UDS или локальный файл. После чего имя используется (если это необходимо, посредством ntxmap), чтобы найти пользователя Windows, а эти учетные данные извлекаются из контроллера домена Windows или базы данных LGDB. Если соответствие не найдено, используются учетные данные пользователя Windows по умолчанию либо в доступе отказывается.

Сведения о Common AntiVirus Agent (CAVA)

Программа Common AntiVirus Agent (CAVA) — антивирусное решение для клиентов, которые используют сервер NAS. В решении используется протокол файловой системы SMB, соответствующий отраслевому стандарту, в среде Microsoft

Windows Server. В средстве CAVA для выявления известных вирусов и предотвращения заражения ими файлов в СХД используется антивирусное программное обеспечение стороннего производителя.

Почему важны антивирусные средства?

Система хранения устойчива к воздействию вирусов благодаря своей архитектуре. Сервер NAS обеспечивает доступ к данным в реальном времени при помощи встроенной операционной системы. Сторонние системы не могут запускать программы, содержащие вирусы, в операционной системе. Хотя ПО операционной системы устойчиво к вирусам, для клиентов Windows, осуществляющих доступ к системе хранения, необходима защита от вирусов. Защита от вирусов на клиенте сокращает шансы того, что клиент разместит зараженный файл на сервере, и обеспечивает защиту клиента в том случае, если на нем будет открыт зараженный файл. В состав антивирусного решения входит ПО операционной системы, агент CAVA и антивирусный модуль стороннего производителя. ПО CAVA и антивирусный модуль стороннего производителя необходимо установить на сервере Windows Server в домене.

Дополнительную информацию об агенте CAVA, который входит в состав Common Event Enabler (CEE), см в разделе *Using the Common Event Enabler on Windows Platforms* по адресу www.dell.com/powerstoredocs.

Подпись программного кода

PowerStore принимает обновления ПО как для новых выпусков, так и для выпусков исправлений. Главный ключ GPG (GNU Privacy Guard) подписывает все пакеты программного обеспечения PowerStore, и Dell EMC контролирует этот ключ GPG. Процесс обновления ПО PowerStore проверяет подпись пакета ПО и отклоняет недействительные подписи, которые могут быть признаком взлома или повреждения. Этап проверки подписи является частью процесса обновления, и подпись пакета ПО проверяется автоматически на этапе подготовки к установке.

2

Настройки безопасности соединения

В этом разделе рассматриваются следующие темы.

Темы:

- Использование портов

Использование портов

В следующих разделах описывается набор сетевых портов и соответствующих сервисов, которые могут присутствовать в устройстве. При определенных обстоятельствах устройство работает в качестве сетевого клиента, например при взаимодействии с сервером vCenter. В этих случаях соединение инициируется устройством, а такие подключения должны поддерживаться сетевой инфраструктурой.

ПРИМЕЧАНИЕ: Дополнительные сведения о портах см. в статье базы знаний 542240, *PowerStore: правила межсетевого экрана в сети заказчика — порты TCP/UDP*. Перейдите к https://www.dell.com/support/kbdoc/en-us/542240. С помощью инструмента «Правила межсетевого экрана в сети заказчика» можно фильтровать и просматривать список правил и портов межсетевого экрана, которые относятся к выполняемому развертыванию PowerStore.

Сетевые порты устройства

В следующей таблице описывается набор сетевых портов и соответствующих сервисов, которые могут присутствовать на устройстве.

Таблица 2. Сетевые порты устройства

Порт	Обслуживание	Протокол	Направление доступа	Описание
22	Клиент SSH, SupportAssist Connect Home	TCP	Двусторонний	• Обеспечивает доступ по SSH (если включен). • Требуется для SupportAssist Connect Home. Если этот порт закрыт, подключения для администрирования по SSH недоступны.
25	SMTP	TCP	Исходящий	Позволяет устройству отправлять сообщения электронной почты. Если закрыт, уведомления по электронной почте будут недоступны.
26	Клиент SSH	TCP	Двусторонний	Доступ по протоколу SSH к порту 22 перенаправляется на этот порт. Если этот порт закрыт, подключения для администрирования по SSH недоступны.
53	DNS	Протокол TCP/UDP	Исходящий	Используется для передачи запросов DNS на сервер DNS. Если закрыт, разрешение имен DNS не будет работать.
80, 8080, 8128	SupportAssist	TCP	Исходящий	Используется для подключения SupportAssist через прокси-сервер.

Таблица 2. Сетевые порты устройства (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
123	NTP	Протокол TCP/UDP	Исходящий	Синхронизация времени по NTP. Если закрыт, синхронизация времени между устройствами не выполняется.
443	HTTPS	TCP	Двусторонний	Безопасная передача трафика HTTP в PowerStore Manager. Если закрыт, соединение с устройством становится недоступным.
500	IPsec (IKEv2)	UDP	Двусторонний	Чтобы межсетевые экраны не препятствовали использованию IPSec, откройте порт UDP 500 и разрешите IP-протоколы с номерами 50 и 51 в фильтрах входящего и исходящего трафика межсетевых экранов. Порт UDP 500 должен быть открыт, чтобы разрешить прохождение трафика по протоколу управления сопоставлением безопасности и криптографическими ключами в Интернете (ISAKMP) через межсетевые экраны. IP-протокол с идентификатором 50 должен быть настроен таким образом, чтобы разрешить прохождение трафика по протоколу безопасной инкапсуляции полезной нагрузки (ESP) из набора IPSec. IP-протокол с идентификатором 51 должен быть настроен таким образом, чтобы разрешить прохождение трафика по протоколу заголовка аутентификации (AH). Если закрыт, подключение IPsec между устройствами PowerStore будет недоступно.
587	SMTP	TCP	Исходящий	Позволяет устройству отправлять сообщения электронной почты. Если закрыт, уведомления по электронной почте будут недоступны.
3033	Импорт	Протокол TCP/UDP	Исходящий	Требуется для импорта хранилища из устаревших систем хранения EqualLogic Peer Storage и Compellent Storage Center.
3260	iSCSI	TCP	• Входящий для доступа хоста и хоста ESXi • Двунаправленный для репликации • Исходящий для импорта хранилища	Требуется для предоставления следующих прав доступа к сервисам iSCSI: • доступ внешнего хоста по протоколу iSCSI; • доступ внешнего или встроенного в PowerStore хоста ESXi по протоколу iSCSI; • межкластерный доступ для репликации; • доступ для импорта хранилища из устаревших систем хранения EqualLogic Peer Storage, Compellent Storage Center, Unity и VNX2. Если этот порт закрыт, сервисы iSCSI будут недоступны. Используется функцией мобильности данных для

Таблица 2. Сетевые порты устройства (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
				поддержки обоснованной производительности репликации при использовании соединения с низкой задержкой.
3261	Мобильность данных	TCP	Двусторонний	Используется мобильностью данных для поддержки обоснованной производительности репликации при подключении с большой задержкой.
5353	DNS многоадресной рассылки (mDNS)	UDP	Двусторонний	Многоадресный запрос DNS. Если закрыт, разрешение имен mDNS не будет работать.
8443	VASA, SupportAssist	TCP	• Входящий для VASA • Исходящий для SupportAssist	• Требуется для поставщика VASA Vendor для VASA 3.0. • Требуется для соответствующих функций SupportAssist Connect Home.
8443, 50443, 55443 или 60443	Агент хоста импорта Windows, агент хоста импорта Linux или агент хоста импорта VMware	TCP	Исходящий	Один из этих портов должен быть открыт при импорте хранилища данных из устаревших систем хранения.
9443	SupportAssist	TCP	Исходящий	Требуется для программного интерфейса REST API SupportAssist, связанного с Connect Home.

Сетевые порты устройства, связанные с файлами

В следующей таблице описывается набор сетевых портов и соответствующих сервисов, которые могут присутствовать на устройстве и связаны с файлами.

ПРИМЕЧАНИЕ: Исходящие порты являются временными.

Таблица 3. Сетевые порты устройства, связанные с файлами

Порт	Обслуживание	Протокол	Направление доступа	Описание
20	FTP	TCP	Исходящий	Порт, используемый для передачи данных по протоколу FTP. Этот порт можно открыть, включив FTP. Аутентификация осуществляется на порту 21 и определяется протоколом FTP.
21	FTP	TCP	Входящий	Порт 21 — это порт управления, на котором сервис FTP прослушивает входящие запросы FTP.
22	SFTP	TCP	Входящий	Разрешает оповещения через SFTP (FTP over SSH). SFTP — это клиент-серверный протокол. Пользователи могут использовать протокол SFTP для передачи файлов на устройство по локальной подсети. Также обеспечивает исходящее соединение по FTP для

Таблица 3. Сетевые порты устройства, связанные с файлами (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
				управления. Если закрыт, FTP недоступен.
53	DNS	Протокол TCP/UDP	Исходящий	Используется для передачи запросов DNS на сервер DNS. Если закрыт, разрешение имен DNS не будет работать. Требуется для SMB v1.
88	Kerberos	Протокол TCP/UDP	Исходящий	Требуется для сервисов аутентификации Kerberos.
111	Привязка RPC (для пространств имен SDNAS; в противном случае — сервис хоста)	Протокол TCP/UDP	Двусторонний	Открывается при помощи стандартного средства portmapper или сервиса rpcbind и является дополнительным сетевым сервисом устройства. Его невозможно остановить. По определению, если клиентская система имеет сетевое подключение к данному порту, она может отправить на него запрос. Аутентификация не требуется.
123	NTP	UDP	Исходящий	Синхронизация времени по NTP. Если закрыт, синхронизация времени между устройствами не выполняется.
135	Microsoft RPC	TCP	Входящий	Различные задачи для MicroSoft Client. Также используется для NDMP.
137	Microsoft Netbios WINS	UDP; TCP/UDP	Входящий; исходящий	Сервис имени NETBIOS связан с сервисами совместного использования файлов SMB на устройстве и является основным компонентом этой функции (Wins). При отключении этого порта отключаются и все связанные с SMB сервисы.
138	Microsoft Netbios BROWSE	UDP	Исходящий	Сервис датаграммы NETBIOS связан с сервисами совместного использования файлов SMB на устройстве и является основным компонентом этой функции. Используется только сервис обзора. Если отключен, этот порт отключает возможность обзора.
139	Microsoft CIFS	TCP	Двусторонний	Сервис сессий NETBIOS связан с сервисами совместного использования файлов SMB на устройстве и является основным компонентом этой функциональной возможности. Когда службы SMB включены, данный порт открыт. Он строго обязателен для SMB v1.
389	LDAP	Протокол TCP/UDP	Исходящий	Незащищенные запросы LDAP. Если закрыт, незащищенные запросы аутентификации LDAP будут недоступны. В качестве альтернативы можно настроить безопасный протокол LDAP.
445	Microsoft SMB	TCP	Входящий	Порт SMB (на контроллере домена) и порт подключений SMB для клиентов Windows 2000 и более поздних версий. Для обеспечения бесперебойной

Таблица 3. Сетевые порты устройства, связанные с файлами (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
				работы требуется сетевое подключение между клиентами с правами доступа к сервисам SMB на устройстве и этим портом. При отключении этого порта отключаются и все связанные с SMB сервисы. Если при этом также отключен порт 139, совместное использование файлов по протоколу SMB также отключается.
464	Kerberos	Протокол TCP/UDP	Исходящий	Требуется для сервисов аутентификации Kerberos и SMB.
500	IPsec (IKEv2)	UDP	Двусторонний	Чтобы межсетевые экраны не препятствовали использованию IPSec, откройте порт UDP 500 и разрешите IP-протоколы с номерами 50 и 51 в фильтрах входящего и исходящего трафика межсетевых экранов. Порт UDP 500 должен быть открыт, чтобы разрешить прохождение трафика по протоколу управления сопоставлением безопасности и криптографическими ключами в Интернете (ISAKMP) через межсетевые экраны. IP-протокол с идентификатором 50 должен быть настроен таким образом, чтобы разрешить прохождение трафика по протоколу безопасной инкапсуляции полезной нагрузки (ESP) из набора IPSec. IP-протокол с идентификатором 51 должен быть настроен таким образом, чтобы разрешить прохождение трафика по протоколу заголовка аутентификации (AH). Если закрыт, подключение IPsec между устройствами PowerStore будет недоступно.
636	протокол LDAPS	Протокол TCP/UDP	Исходящий	Защищенные запросы LDAP. Если закрыт, защищенная аутентификация LDAP будет недоступна.
1234	NFS mountd	Протокол TCP/UDP	Двусторонний	Используется для работы сервиса монтирования, который является основным компонентом сервиса NFS (версий 2, 3 и 4).
2000	SSHD	TCP	Входящий	SSHD для удобства обслуживания (опция)
2049	Операции ввода-вывода NFS	Протокол TCP/UDP	Двусторонний	Используется для работы служб NFS.
3268	LDAP	UDP	Исходящий	Незащищенные запросы LDAP. Если закрыт, незащищенные запросы аутентификации LDAP будут недоступны.
4000	STATD для NFSv3	Протокол TCP/UDP	Двусторонний	Используется для предоставления сервисов NFS statd. statd — это средство мониторинга состояния блокировки файлов NFS, который вместе с lockd предоставляет NFS

Таблица 3. Сетевые порты устройства, связанные с файлами (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
				функции восстановления после сбоев. Если этот порт закрыт, службы NAS statd будут недоступны.
4001	NLMD для NFSv3	Протокол TCP/UDP	Двусторонний	Используется для предоставления сервисов NFS lockd. lockd — управляющая программа блокировки файлов NFS. Она обрабатывает запросы на блокировку от клиентов NFS и работает вместе с управляющей программой statd. Если этот порт закрыт, службы NAS lockd будут недоступны.
4002	RQUOTAD для NFSv3	TCP/UDP; UDP	Входящий; исходящий	Используется для предоставления служб NFS rquotad. Управляющая программа rquotad предоставляет информацию о квотах клиентам NFS, смонтировавшим файловую систему. Если этот порт закрыт, службы NAS rquotad будут недоступны.
4003	XATTRPD (дополнительный атрибут файла)	Протокол TCP/UDP	Входящий	Требуется для управления атрибутами файлов в многопротокольной инфраструктуре.
4658	PAX (архив сервера NAS)	TCP	Входящий	PAX — это протокол архивов устройства, который работает со стандартными форматами лент UNIX.
8888	RCPD (путь прохождения данных репликации)	TCP	Входящий	Используется репликатором (на вторичной стороне). Открывается репликатором при необходимости репликации данных. Если служба запущена, ее невозможно остановить.
10000	NDMP	TCP	Входящий	• Позволяет управлять резервным копированием и восстановлением, которые выполняются на сервере протокола управления сетевыми данными (NDMP), через приложение сетевого резервного копирования, не требуя установки на сервере ПО стороннего производителя. На устройстве сервер NAS выполняет функции сервера NDMP. • Служба NDMP может быть отключена, если ленточный накопитель для резервного копирования NDMP не используется. • В службе NDMP аутентификация выполняется с помощью имени пользователя и пароля. Имя пользователя можно настроить. В документации по NDMP описывается процедура настройки пароля для широкого спектра сред.
[10500,10531]	Зарезервированный диапазон NDMP для динамических портов NDMP	TCP	Входящий	Для сессий трехстороннего резервного копирования или восстановления серверы NAS используют порты от 10500 до 10531.

Таблица 3. Сетевые порты устройства, связанные с файлами (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
12228	Сервис антивирусной проверки	TCP	Исходящий	Требуется для сервиса антивирусной проверки.

Сетевые порты, связанные с устройствами модели PowerStore X

В следующей таблице описывается набор сетевых портов и соответствующих сервисов, которые могут присутствовать на устройствах PowerStore X model.

Таблица 4. Сетевые порты, связанные с устройствами PowerStore X model

Порт	Обслуживание	Протокол	Направление доступа	Описание
22	Сервер SSH	TCP	Входящий	Обеспечивает доступ по SSH (если включен). Если этот порт закрыт, подключения для администрирования по SSH недоступны.
80, 9000	vSphere Web Access	TCP	Входящий	Доступ для подключаемого модуля веб-клиента vSphere Update Manager для веб-клиента vSphere Web Client.
427	Протокол обнаружения сервисов (SLP) CIM	Протокол TCP/UDP	Двусторонний	Клиент CIM использует протокол SLPv2 (Service Location Protocol, версия 2) для поиска серверов CIM.
443	Веб-клиент vSphere Web Client	TCP	Входящий	Используется для клиентских подключений.
902	Копия сетевого файла (NFC), VMware vCenter, веб-клиент vSphere Web Client	TCP	• Двунаправленный для NFC • Исходящий для VMware vCenter • Входящий для веб-клиента vSphere Web Client	• NFC предоставляет сервис FTP с распознаванием типов файлов для компонентов vSphere. ESXi использует NFC для таких операций, как копирование и перемещение данных между хранилищами данных по умолчанию. • Агент VMware vCenter • Для веб-клиента vSphere Web Client, используется для клиентских подключений.
5900, 5901, 5902, 5903, 5904	Протокол RFB	TCP	Входящий	Удаленный доступ к графическим интерфейсам пользователя, таким как VNC.
5988	Сервер CIM (Common Information Model)	TCP	Входящий	Сервер для CIM.
5989	Безопасный сервер CIM	TCP	Входящий	Сервер для CIM.
6999	Виртуальный распределенный логический маршрутизатор NSX, rabbitmqproxy	UDP	• Двунаправленный для сервиса виртуального распределенно	• В случае сервиса виртуального распределенного маршрутизатора NSX порт межсетевого экрана, связанный с этим сервисом,

Таблица 4. Сетевые порты, связанные с устройствами PowerStore X model (продолжение)

Порт	Обслуживание	Протокол	Направление доступа	Описание
			го маршрутизатора NSX • Исходящий для rabbitmqproxy	открывается, когда устанавливаются VIB NSX и создается модуль VDR. Если с хостом не связано ни одного экземпляра VDR, порт открывать необязательно. • В случае rabbitmqproxy: прокси-сервер, работающий на хосте ESXi. Этот прокси-сервер позволяет приложениям, работающим на виртуальных машинах, обмениваться данными с брокерами AMQP, которые работают в сетевом домене vCenter. Подключение виртуальной машины к сети необязательно, т. е. сетевая плата не требуется. Убедитесь, что IP-адреса исходящих соединений включают по крайней мере используемые или будущие брокеры. Брокеры можно добавить позже при расширении системы.
8000	vMotion	TCP	Двусторонний	Требуется для переноса виртуальной машины с помощью vMotion. Хосты ESXi прослушивают порт 8000 для обнаружения соединений по протоколу TCP от удаленных хостов ESXi для передачи данных vMotion.
8100, 8200, 8300	Отказоустойчивость	Протокол TCP/UDP	Двусторонний	Используется для передачи данных между хостами для vSphere Fault Tolerance (FT).
8301, 8302	DVSSync	UDP	Двусторонний	Порты DVSSync используются для синхронизации состояний распределенных виртуальных портов между хостами, для которых активированы запись/воспроизведение VMware FT. Эти порты должны быть открыты только на хостах, на которых работают основные или резервные виртуальные машины. На хостах, не использующих VMware FT, эти порты открывать необязательно.
9080	Фильтр операций ввода-вывода	TCP	Исходящий	Используется функцией фильтра операций ввода-вывода хранилища.
31031	vSphere Replication, VMware Site Recovery Manager	TCP	Исходящий	Используется vSphere Replication и VMware Site Recovery Manager для трафика текущей репликации.
44046	vSphere Replication, VMware Site Recovery Manager	TCP	Исходящий	Используется vSphere Replication и VMware Site Recovery Manager для трафика текущей репликации.

3

Аудит

В этой главе содержится следующая информация:

Темы:

Контроль

Контроль обеспечивает историческое представление действий пользователей в системе. Пользователь с ролью администратора, администратора безопасности или администратора хранилища может использовать программный интерфейс REST API для поиска и просмотра событий изменения конфигурации в системе. В рамках аудита проверяются не только события, связанные с безопасностью. В журналах аудита также регистрируются все операции настройки (т. е. POST/PATCH/DELETE).

Для поиска и просмотра событий аудита можно использовать и другие интерфейсы, например пользовательский интерфейс PowerStore Manager или интерфейс командной строки.

4

Параметры безопасности данных

В этом разделе рассматриваются следующие темы.

Темы:

Шифрование данных в состоянии покоя

Для основного хранилища (твердотельных накопителей NVMe, накопителей ПНК NVMe и твердотельных накопителей SAS) в PowerStore применяется шифрование данных в состоянии покоя (D@RE) с использованием самошифруемых накопителей (SED) в соответствии со стандартом FIPS 140-2. Устройство кэширования NVRAM шифруется, но в настоящее время соответствие стандарту FIPS 140-2 не подтверждено.

Шифрование выполняется на каждом из дисков перед записью данных на носитель. Это защищает данные на диске от хищения или потери, а также от попыток прочитать диск напрямую путем его физического деконструирования. Кроме того, шифрование позволяет быстро и безопасно стереть информацию с диска таким образом, чтобы ее невозможно было восстановить. Помимо защиты от угроз, связанных с физическим удалением носителей, носители можно быстро перепрофилировать путем удаления ключа шифрования, который используется для обеспечения безопасности данных, хранившихся на этом носителе ранее.

Для чтения зашифрованных данных требуется ключ аутентификации, позволяющий разблокировать диск SED. Доступ возможен только к разблокированным дискам SED, прошедшим аутентификацию. После выполнения разблокировки диск SED расшифровывает зашифрованные данные, восстанавливая их первоначальную форму.

Все диски на устройстве PowerStore должны быть дисками SED. Если вы попытаетесь добавить несамошифруемый диск на устройство, возникнет ошибка. Кроме того, не поддерживается использование незашифрованных устройств в зашифрованном кластере.

Активация шифрования

Функция шифрования данных в состоянии покоя на устройствах PowerStore настраивается изготовителем. Во всех странах, в которых разрешен импорт устройств с поддержкой шифрования, шифрование включено по умолчанию. Если шифрование включено, отключить его невозможно. Во всех странах, в которых запрещен импорт устройств с поддержкой шифрования, функция шифрования данных в состоянии покоя отключена по умолчанию.

ПРИМЕЧАНИЕ: Устройства, не поддерживающие шифрование данных в состоянии покоя, нельзя использовать в одном кластере с зашифрованными устройствами.

состояние шифрования;

Состояние шифрования для устройства отображается на следующих уровнях:

- уровень кластера;
- уровень устройства;

- уровень накопителя.

Состояние шифрования на уровне кластера отражает лишь то, включено ли шифрование для устройства. Оно никак не связано с состоянием накопителя.

Состояние шифрования устройства может иметь одно из следующих значений:

- Encrypted — возможность шифрования на устройстве включена.
- Unencrypted — возможность шифрования не поддерживается устройством.
- Encrypting — отображается в процессе активации шифрования. После успешного завершения процесса шифрования состояние шифрования на уровне кластера отображается как «encrypted».

Состояние шифрования на уровне накопителя предоставляется каждому накопителю устройства и может иметь одно из следующих значений:

- Encrypted — накопитель зашифрован. Это обычное состояние накопителя на устройстве, которое поддерживает шифрование.
- Encrypting — устройство включает возможность шифрования на накопителе. Это состояние может отображаться во время начальной активации шифрования на устройстве или при добавлении новых накопителей на настроенное устройство.
- Disabled — нельзя включить шифрование для накопителя из-за ограничений на импорт, действующих в определенной стране. Если какой-либо из накопителей находится в этом состоянии, все накопители в кластере также будут отображаться в этом состоянии.
- Unknown — устройство еще не попыталось включить шифрование на накопителе. Это состояние может отображаться во время начальной активации шифрования на устройстве или при добавлении новых накопителей на настроенное устройство.
- Unsupported — накопитель не поддерживает шифрование.
- Foreign — накопитель поддерживается, но заблокирован другим устройством. Для использования на этом устройстве накопитель необходимо списать.

Управление ключами

Сервис встроенного диспетчера ключей (KMS) запускается на активном узле каждого устройства PowerStore. Этот сервис управляет защищенным хранилищем файла локального хранилища ключей для обеспечения автоматического резервного копирования ключей шифрования на системные и загрузочные накопители. Он также осуществляет управление процессом блокировки и разблокировки самошифруемого диска (SED) и отвечает за управление локальным хранилищем ключей на устройстве. Файл локального хранилища ключей шифруется с применением 256-разрядного ключа AES, а для защищенного хранилища файла хранилища ключей используется технология BSAFE от RSA.

KMS автоматически создает случайный ключ аутентификации для диска SED во время инициализации устройства. У всех дисков (включая добавленные на устройство позже) есть уникальный ключ аутентификации, который используется в процессах блокировки и разблокировки дисков SED. Ключ шифрования ключей применяется для шифрования ключей аутентификации и шифрования в хранилище файла хранилища ключей и в устройстве в процессе его эксплуатации. Ключи шифрования носителей хранятся на выделенных дисках SED, и доступ к ним невозможен. Когда шифрование включено, все ключи аутентификации хранятся на устройстве.

Файл резервной копии хранилища ключей

KMS поддерживает создание и скачивание резервной копии архивного файла хранилища ключей на устройстве в автономном режиме. Резервное копирование устройства в автономном режиме уменьшает шансы потери ключа в результате аварии, из-за чего использование устройства или кластера может стать невозможным. Если в момент инициации резервного копирования хранилища ключей кластера какое-либо устройство недоступно, операция будет выполнена, однако при этом отобразится предупреждение, что в резервной копии содержатся файлы хранилища ключей не для всех устройств в кластере и операцию необходимо выполнить повторно, когда устройство в автономном режиме снова будет доступно.

ПРИМЕЧАНИЕ: Главное устройство в кластере содержит архивный файл хранилища ключей кластера, который включает резервные копии хранилищ ключей из каждого устройства, обнаруженного в кластере, включая главное устройство.

При изменении конфигурации системы в кластере изменения вносятся и в хранилище ключей, поэтому в этом случае рекомендуется создать новый архивный файл хранилища ключей для скачивания. Одновременно можно запустить только одну операцию скачивания резервной копии архивного файла хранилища ключей.

ПРИМЕЧАНИЕ: Настоятельно рекомендуется скачивать созданный архивный файл хранилища ключей во внешнее, безопасное расположение. Если файлы хранилища ключей в системе повреждаются и становятся недоступными, система переходит в режим обслуживания. Для решения этой проблемы потребуется архивный файл хранилища ключей и договор на обслуживание.

Для резервного копирования архивного файла хранилища ключей пользователь должен обладать ролью администратора или администратора хранилища. Чтобы выполнить резервное копирование архивного файла хранилища ключей, нажмите **Settings** и в разделе **Security** выберите **Encryption**. На странице **Encryption** в разделе **Lockbox Backup** нажмите **Download Keystore Backup**.

ПРИМЕЧАНИЕ: Чтобы восстановить хранилище ключей из резервной копии в случае сбоя, обратитесь к поставщику услуг.

Изменение назначения диска на устройстве с включенным шифрованием

Об этой задаче

Самошифруемый диск (SED) блокируется, когда устройство инициализировано или когда он вставляется в уже инициализированное устройство. Диск нельзя использовать в другой системе без предварительной разблокировки. Заблокированный диск становится непригодным для использования в другом устройстве, а его состояние шифрования отображается как `Foreign` в новом устройстве. Диск можно назначить для нового устройства, однако все существующие данные на нем будут утрачены.

Для изменения назначения диска с состоянием шифрования `Foreign` на устройстве выполните следующие действия:

Действия

1. Запишите идентификатор физической защиты (PSID), указанный на этикетке с тыльной стороны накопителя. PSID потребуется указать в рамках процесса по изменению назначения.
2. В PowerStore Manager щелкните **Hardware**, выберите устройство и затем карточку **Hardware**.
3. Выберите диск для изменения назначения.

   В строке **Encryption Status** для диска должно отображаться значение `Foreign`.
4. Щелкните **Repurpose Drive**.
   Отобразится слайд **Repurpose Drive**.
5. Введите PSID диска и щелкните **Apply**.

Результат

Диск отобразится на устройстве в качестве нового диска, а его состояние шифрования изменится на `Encrypted` после завершения процесса изменения назначения.

Замена базового шасси и узлов в системе с включенным шифрованием

Для замены base enclosure и nodes на устройстве с включенным шифрованием требуется договор на обслуживание.

Восстановление заводских настроек устройства

Сервисный скрипт `svc_factory_reset` возвращает кластер с одним устройством в состояние заводской поставки, удаляя все пользовательские данные и постоянные конфигурации.

В случае кластеров с несколькими устройствами скрипт `svc_factory_reset` не может выполняться на вторичных устройствах. Вместо него должен использоваться скрипт `svc_remove_appliance`. Этот скрипт возвращает вторичное

устройство в состояние заводской поставки, удаляя все пользовательские данные и постоянные конфигурации. Если в кластере осталось только главное устройство, для сброса этого устройства можно выполнить скрипт `svc_factory_reset`.

ПРИМЕЧАНИЕ: Рекомендуется, чтобы эти скрипты запускались только квалифицированным поставщиком услуг.

Дополнительную информацию об этих скриптах см. в документе*PowerStore Service Scripts Guide*.

5

Настройки безопасного удобства обслуживания

В этой главе содержится следующая информация:

Темы:

Описание использования SupportAssist™

Функция SupportAssist обеспечивает IP-подключение, позволяющее службе поддержки Dell EMC Support получать файлы ошибок и оповещения от вашего устройства и удаленно осуществлять поиск и устранение неисправностей, благодаря чему повышаются оперативность и эффективность решения проблем.

ПРИМЕЧАНИЕ: Настоятельно рекомендуется активировать функцию SupportAssist для ускорения диагностики проблем, поиска неполадок и сокращения времени их устранения. Если функция SupportAssist отключена, вам может потребоваться вручную собрать сведения об устройстве, чтобы помочь службе поддержки Dell EMC Support в поиске и устранении неполадок, а также в разрешении проблем с вашим устройством. Кроме того, функция SupportAssist должна быть включена на устройстве для передачи данных в CloudIQ. Информацию о CloudIQ см. на странице www.dell.com/support. После выполнения входа найдите страницу **Product Support** для CloudIQ.

SupportAssist и безопасность

Функция SupportAssist использует несколько уровней безопасности на каждом этапе процесса удаленного подключения, чтобы и вы, и специалисты Dell EMC могли безопасно использовать это решение.

- Все уведомления в службу поддержки Dell EMC отправляются исключительно с вашей площадки и никогда не отправляются откуда-либо извне. Безопасность обеспечивается при помощи 256-разрядного алгоритма шифрования AES.
- Архитектура на базе протокола IP интегрируется с уже имеющейся у вас инфраструктурой и поддерживает безопасность вашей среды.
- Соединение между вашей площадкой и службой поддержки Dell EMC защищено с помощью двусторонней аутентификации с использованием цифровых сертификатов RSA®.
- Только авторизованные специалисты по обслуживанию клиентов Dell EMC, прошедшие проверку посредством двухфакторной аутентификации, могут скачивать цифровые сертификаты, необходимые для просмотра уведомлений с вашей площадки.
- Дополнительное приложение диспетчера политик в SupportAssist v3 позволяет разрешать или запрещать доступ службы поддержки Dell EMC Support на основе ваших собственных уникальных правил и требований и включает подробный журнал аудита.

Управление SupportAssist

Функцией SupportAssist можно управлять с помощью PowerStore Manager или программного интерфейса REST API. Вы можете активировать или отключать сервис и предоставлять актуальную информацию, необходимую для выбранного вами варианта SupportAssist.

ПРИМЕЧАНИЕ: Варианты **Gateway Connect with remote assist** и **Gateway Connect without remote assist** для централизованного SupportAssist не поддерживают высокую доступность (HA). Эти варианты не предоставляют возможности аварийного переключения на активный кластер SupportAssist высокой доступности. При развертывании устройства PowerStore на одном сервере шлюза высокой доступности, который является единственным вариантом конфигурации, переключение на работоспособный сервер шлюза в кластере невозможно. Если сервер шлюза высокой доступности, к которому подключено устройство, отключается, устройство прекращает передачу в службу поддержки Dell EMC всех исходящих файлов, таких как файлы функции «звонок домой» и файлы CloudIQ. Подключение SupportAssist для входящих данных в рамках удаленного доступа к устройству будет по-прежнему работать с использованием работоспособного сервера шлюза высокой доступности в кластере. Кроме того, варианты SupportAssist **Gateway Connect with remote assist** и **Gateway Connect without remote assist** следует настраивать только на назначенном для этой цели главном устройстве системы.

Само по себе устройство не применяет какие-либо политики. Если вам необходим усиленный контроль над удаленным доступом к устройству, можно назначить разрешения доступа с помощью диспетчера политик. Программный компонент диспетчера политик можно установить на сервере заказчика. Он управляет удаленным доступом к устройствам, ведет журнал аудита удаленных подключений и обеспечивает операции передачи файлов. Можно контролировать, кто получает доступ к устройству, к каким его компонентам и когда. Для получения дополнительной информации о диспетчере политик перейдите по адресу www.dell.com/support. После выполнения входа перейдите на подходящую страницу **Support by Product** и найдите ссылку на необходимую техническую документацию по интересующему вас продукту SupportAssist.

Соединение SupportAssist

ПРИМЕЧАНИЕ: SupportAssist невозможно активировать в моделях PowerStore, для которых настроено использование IPv6 для сети управления. SupportAssist не поддерживает IPv6. Кроме того, если для кластера настроена функция SupportAssist, система не позволит перенастроить сеть управления с IPv4 на IPv6.

Для работы функции SupportAssist требуется доступ к DNS-серверу.

Connection Status в SupportAssist показывает состояние соединения между PowerStore и внутренними сервисами поддержки Dell EMC, а также качество обслуживания для данного соединения. Состояние соединения определяется за пятиминутные периоды, а качество обслуживания для соединения определяется за 24-часовые периоды. Для соединения может указываться одно из приведенных ниже значений **Connection Status** в зависимости от состояния любого из устройств в кластере:

- `Unavailable` – Данные о возможности подключения недоступны. Возможно, связь с устройством утрачена либо функция SupportAssist только что активирована и еще недостаточно данных для определения состояния.
- `Disabled` – Функция SupportAssist не активирована.
- `Not connected` – Возможность подключения утрачена. Пять раз подряд произошел сбой функции KeepAlive.
- `Reconnecting` – PowerStore пытается восстановить соединение после потери возможности подключения. Для возврата в состояние «подключено» требуется, чтобы пять раз подряд успешно завершился запрос KeepAlive.

Для соединения может указываться одно из приведенных ниже значений **Connection Status** на основе усреднения по всем устройствам в кластере, когда PowerStore подключен к внутренним сервисам поддержки Dell EMC:

- `Evaluating` — В течение первых 24 часов после первой инициализации SupportAssist качество обслуживания для соединения еще не будет определено.
- `Good` — Не менее 80 % последовательных запросов KeepAlive были успешными.
- `Fair` — От 50 % до 80 % последовательных запросов KeepAlive были успешными.
- `Poor` — Менее 50 % последовательных запросов KeepAlive были успешными.

Варианты SupportAssist

Функция SupportAssist обеспечивает IP-подключение, позволяющее службе поддержки Dell EMC Support получать файлы ошибок и оповещения от вашей системы и удаленно осуществлять поиск и устранение неисправностей, благодаря чему повышаются оперативность и эффективность решения проблем.

Доступны следующие варианты SupportAssist, которые можно использовать для отправки сведений об устройствах в службу поддержки Dell EMC Support для удаленного поиска и устранения неисправностей:

- Gateway Connect without remote access — для централизованной функции SupportAssist, которая работает на предоставляемом заказчиком сервере шлюза, с двунаправленной передачей файлов, что включает:
  - функцию «звонок домой»;
  - поддержку CloudIQ;
  - уведомления программного обеспечения;
  - скачивание операционных сред или микропрограмм со страницы Dell EMC Support в кластер.

  Сервер шлюза SupportAssist — это единая точка входа и выхода для всех действий SupportAssist на базе IP-подключения для устройств, связанных со шлюзом.
- Gateway Connect with remote access — для централизованной функции SupportAssist, которая работает на предоставляемом заказчиком сервере шлюза, с двунаправленной передачей тех же файлов, что и при варианте Gateway Connect without remote access, и удаленным доступом для сотрудников службы поддержки Dell EMC Support.
- Direct Connect without remote access — для распределенной функции SupportAssist, которая работает на отдельных устройствах, с двунаправленной передачей тех же файлов, что и при варианте Gateway Connect without remote access.
- Direct Connect with remote access — для распределенной функции SupportAssist, которая работает на отдельных устройствах, с двунаправленной передачей тех же файлов, что и при варианте Gateway Connect without remote access, и удаленным доступом для сотрудников службы поддержки Dell EMC Support.

Также доступен вариант Disabled, но его использовать не рекомендуется. Если вы выберете этот вариант, служба поддержки Dell EMC не будет получать уведомления о проблемах, возникающих на вашем устройстве. Вам может потребоваться собрать сведения об устройстве вручную, чтобы помочь представителям службы поддержки в поиске и устранении неисправностей, а также в разрешении проблем с устройством.

Параметры SupportAssist Gateway Connect

SupportAssist Gateway Connect работает на сервере шлюза. Если выбран вариант **Gateway Connect without remote access** или **Gateway Connect with remote access**, устройство добавляется к другим устройствам в кластере SupportAssist. Этот кластер находится за одним общим (централизованным) безопасным подключением между серверами службы поддержки Dell EMC и автономным сервером шлюза. Сервер шлюза представляет собой единую точку входа и выхода для всех действий Dell EMC SupportAssist на базе IP-подключения для устройств, связанных с этим шлюзом.

Сервер шлюза — это решение для удаленной поддержки, которое устанавливается на один или несколько выделенных серверов, предоставляемых заказчиком. Сервер шлюза функционирует в качестве посредника по обмену данными между связанными устройствами и компанией Dell EMC.

Дополнительную информацию о SupportAssist Gateway можно найти на странице продукта SupportAssist на веб-сайте Dell Support (www.dell.com/support).

Чтобы настроить устройство для использования варианта **Gateway Connect without remote access** или **Gateway Connect with remote access** для SupportAssist, необходимо указать IP-адрес и номер порта (по умолчанию 9443) сервера шлюза. Кроме того, убедитесь, что открыт порт между сервером шлюза и устройством.

ПРИМЕЧАНИЕ: Сервер шлюза должен быть запущен до начала настройки его использования на устройстве. Устройства могут быть добавлены в шлюз только из PowerStore Manager. Если устройство добавлено с сервера шлюза, оно будет отображаться как подключенное, но не сможет отправлять системную информацию.

Параметры SupportAssist Direct Connect

SupportAssist Direct Connect запускается непосредственно на первичном узле каждого устройства. В кластере каждое устройство будет устанавливать собственное соединение с Dell EMC Support. Трафик не направляется через главное устройство в кластере. Тем не менее, осуществлять управление SupportAssist можно только на уровне кластера, то есть все изменения применяются ко всем устройствам в кластере.

Активируйте и настройте SupportAssist Direct Connect на странице **Support Assist**, которую можно открыть с помощью **Settings** и которая указана в списке в разделе **Support** в PowerStore Manager. В результате этих действий устройство будет настроено так, чтобы использовать для подключения к службе поддержки Dell EMC Support защищенное соединение. Для SupportAssist Direct Connect можно выбрать один из следующих вариантов подключения для удаленного обслуживания.

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Если выбран параметр **Direct Connect without remote access** и приняты условия лицензионного соглашения с конечным пользователем (EULA), устройство устанавливает безопасное соединение между собой и Dell EMC Support. Этот параметр обеспечивает возможности подключения для двусторонней передачи файлов в службу Dell EMC Support и из нее. Если это применимо, можно настроить подключение устройства к связанному прокси-серверу (необязательно). При необходимости вы можете позднее обновить Direct Connect до версии с настройкой конфигурации удаленного доступа.

Если выбран параметр **Direct Connect with Remote Access** и приняты условия лицензионного соглашения с конечным пользователем (EULA), устройство устанавливает безопасное соединение между собой и Dell EMC Support. Этот параметр обеспечивает возможности подключения для обслуживания с удаленным доступом между устройством и Dell EMC Support, а также для двусторонней передачи файлов. Если это применимо, можно настроить подключение устройства к диспетчеру политик (необязательно) и любому из связанных прокси-серверов (необязательно) с помощью PowerStore Manager.

При добавлении нового устройства в существующий кластер новое устройство обнаружит настройки SupportAssist кластера и автоматически настроится под них. Если в данный момент активирована функция SupportAssist Direct Connect, она будет автоматически активирована в новом устройстве. Дополнительные действия не требуются. Если SupportAssist Direct Connect активировать невозможно, это не помешает выполнить процедуру добавления устройства.

Требования для SupportAssist Gateway Connect

При реализации вариантов SupportAssist **Gateway Connect without remote access** и **Gateway Connect with remote access** должны выполняться следующие требования:

- На порте 9443 (или на порте, указанном заказчиком, если он отличается) должен быть разрешен сетевой трафик (HTTPS) между устройством и сервером SupportAssist Gateway.
- Требуется SupportAssist версии 4.0.5 или 3.38.

ПРИМЕЧАНИЕ: Никогда не добавляйте устройство на сервер шлюза и не удаляйте его с сервера вручную. Добавляйте устройство на сервер шлюза и удаляйте его с сервера шлюза только с помощью мастера настройки PowerStore Manager SupportAssist.

Требования для SupportAssist Direct Connect

При реализации вариантов SupportAssist **Direct Connect without remote access** и **Direct Connect with remote access** должно выполняться следующее требование:

- Сетевой трафик (HTTPS) должен быть разрешен на портах 443 и 8443 (исходящий) в направлении службы поддержки Dell EMC. Если порт 8443 не будет открыт, это приведет к значительному воздействию на производительность (30–45%). Игнорирование требования открыть оба порта может привести к задержке в устранении проблем с конечным устройством.

Следующее требование должно выполняться только при реализации варианта SupportAssist **Direct Connect with Remote Access**:

- Если в вашей реализации для усиления контроля над удаленным доступом к устройству планируется использовать диспетчер политик, это необходимо указать при настройке функции SupportAssist.

Настройка SupportAssist

Настройте SupportAssist для устройства с помощью любого из следующих средств:

- Мастер начальной настройки — пользовательский интерфейс для пошаговой начальной настройки PowerStore Manager и подготовки системы к использованию.
- **Suppoprt Assist** — страница параметров, доступ к которой возможен из PowerStore Manager (нажмите **Settings** и в разделе **Support** выберите **SupportAssist**).

- Сервер REST API — прикладной интерфейс, который может принимать запросы REST API для настройки параметров SupportAssist. Дополнительные сведения о REST API см. в документе PowerStore REST API Reference Guide.

Чтобы определить состояние функции SupportAssist, нажмите **Settings** в PowerStore Manager и в разделе **Support** выберите **SupportAssist**.

Настройка SupportAssist

Об этой задаче

Чтобы настроить SupportAssist с помощью PowerStore Manager, выполните следующее:

ПРИМЕЧАНИЕ: Для изменения варианта **Direct Connect with remote access** на вариант **Direct Connect without remote access** или **Gateway Connect** потребуется помощь специалистов службы поддержки Dell EMC.

Действия

1. Щелкните **Settings** и в разделе **Settings** выберите **SupportAssist**.
2. Если для SupportAssist отображается отключенное состояние, нажмите значок элемента управления **SupportAssist**, чтобы активировать SupportAssist.

   Функцию SupportAssist можно отключить, однако делать это не рекомендуется.

   Кнопка должна переместиться вправо, а надпись на ней должна поменяться на `Enabled`. Однако **Connection Status** не изменится до тех пор, пока вы не введете необходимую информацию о конфигурации и не нажмете **Apply**.
3. В разделе **SupportAssist** флажок **Connect to CloudIQ** выбран по умолчанию. Если вы не хотите отправлять файлы в CloudIQ, снимите флажок; в противном случае оставьте его.
4. В списке **Type** выберите тип варианта SupportAssist, который вы хотите использовать.
5. В зависимости от выбранного типа варианта SupportAssist выполните одно из следующих действий:
   - Для любого из вариантов **Gateway Connect without remote access** и **Gateway Connect with remote access**:
     - Укажите IP-адрес сервера шлюза.

       ПРИМЕЧАНИЕ: Сервер шлюза должен быть запущен до начала настройки его использования на устройстве.
     - Если порт, который будет использоваться для подключения к серверу шлюза, отличается от значения по умолчанию (9443), с помощью элементов управления выберите номер порта, который будет использоваться в вашей сети.
   - Для варианта **Direct Connect without remote access**:
     - Если ваше сетевое подключение использует прокси-сервер, укажите IP-адрес прокси-сервера.

       ПРИМЕЧАНИЕ: Прокси-сервер должен быть запущен до начала настройки его использования в системе.
     - С помощью элементов управления выберите номер порта, который будет использоваться для подключения к прокси-серверу в вашей сети.
   - Для варианта **Direct Connect with Remote Access**:
     - Если ваше сетевое подключение использует прокси-сервер, укажите IP-адрес прокси-сервера.

       ПРИМЕЧАНИЕ: Прокси-сервер должен быть запущен до начала настройки его использования на устройстве.
     - С помощью элементов управления выберите номер порта, который будет использоваться для подключения к прокси-серверу в вашей сети.
     - Если вы собираетесь использовать диспетчер политик для управления удаленным доступом к вашей системе, укажите IP-адрес диспетчера политик.

       ПРИМЕЧАНИЕ: Диспетчер политик должен быть запущен до начала настройки его использования на устройстве.
     - Если порт, который будет использоваться для подключения к диспетчеру политик, отличается от значения по умолчанию (9443), введите номер порта, который будет использоваться в вашей сети.
6. В зависимости от выбранного типа варианта SupportAssist выполните одно из следующих действий:
   - Для любого из вариантов **Direct Connect without remote access** и **Direct Connect with Remote Access** перейдите к следующему шагу.
   - Для любого из вариантов **Gateway Connect without remote access** и **Gateway Connect with Remote Access** выберите **Test Connection**, чтобы проверить состояние подключения к серверу шлюза.

ПРИМЕЧАНИЕ: Если в поле «Connectivity Status» сохраняется значение `Transitioning` и не меняется в течение нескольких минут (времени, достаточного для проверки возможности подключения), обратитесь в службу онлайн-поддержки.

7. Выберите **Send Test Alert**, чтобы отправить тестовое оповещение в службу поддержки Dell EMC и убедиться в наличии сквозного соединения.
8. Убедитесь в том, что указана правильная контактная информация. Исправьте все неправильные и устаревшие сведения.

   Контактная информация в SupportAssist критически важна для быстрого реагирования на проблемы, требующие участия службы поддержки, и должна быть точной и актуальной.
9. Выберите **Apply**, чтобы сохранить сведения о конфигурации SupportAssist.

A

Пакеты шифрования TLS

В этом приложении содержится следующая информация:

Темы:

- Поддерживаемые пакеты шифрования TLS

Поддерживаемые пакеты шифрования TLS

Пакет шифрования определяет набор методов защиты передачи данных по протоколу TLS.

- Алгоритм обмена ключами (каким образом секретный ключ, используемый для шифрования данных, передается с клиента на сервер). Примеры: ключ RSA или Diffie-Hellman (DH).
- Метод аутентификации (каким образом хосты могут аутентифицировать удостоверения удаленных хостов). Примеры: сертификат RSA, сертификат DSS или без аутентификации.
- Шифр шифрования (способ шифрования данных). Примеры: AES (256- или 128-разрядный).
- Алгоритм хэширования (защита данных за счет обеспечения способа проверки неизменности данных). Примеры: SHA-2 или SHA-1.

Поддерживаемые пакеты шифрования объединяют все эти составляющие.

В следующем списке указаны принятые в OpenSSL имена пакетов шифрования TLS для устройства, а также соответствующие порты.

Таблица 5. Используемые по умолчанию / поддерживаемые на устройстве пакеты шифрования TSL

Пакеты шифрования	Протоколы	Порты
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443