HP Data Protector for PCs 7.0 Руководство по установке и администрированию

Обозначение: н/д
Опубликовано: июнь 2011 г.
Редакция Первая

Оглавление

Сведения о руководстве

В настоящем руководстве рассматриваются следующие вопросы:

- установка HP Data Protector for PCs;
- настройка политик HP Data Protector for PCs;
- программное обеспечение (ПО) агента HP Data Protector for PCs на настольных и переносных компьютерах пользователей;
- определение количества поддерживаемых агентов;
- получение технической поддержки для Data Protector for PCs.

Целевая аудитория

Настоящее руководство предназначено для администраторов, планирующих установку и настройку HP Data Protector for PCs. Желательно иметь некоторые знания в следующих областях:

- администрирование Windows.

Соглашения и обозначения, принятые в документе

Соглашение	**Элемент**
Текст, выделенный синим цветом: «Сведения о руководстве» [5]	Перекрестные ссылки и адреса электронной почты
Подчеркнутый текст, выделенный синим цветом: http://www.hp.com	Адреса веб-сайтов
Полужирный текст	• Нажимаемые клавиши • Текст, вводимый в элемент графического интерфейса, например поле • Элементы графического интерфейса, которые нажимаются или выбираются, например пункты меню и списков, кнопки, вкладки и флажки
Курсивный текст	Выделенный текст

Соглашение	Элемент
Моноширинный текст	• Имена файлов и каталогов • Выходные данные системы • Код • Команды, их аргументы и значения аргументов
Моноширинный курсивный текст	• Переменные в коде • Переменные в командах
Моноширинный полужирный текст	Выделенный моноширинный текст

ВАЖНО Поясняющая информация или специальные инструкции.

ПРИМЕЧАНИЕ Дополнительные сведения.

Общие сведения

Общие сведения о Data Protector for PCs см. на веб-сайте http://www.hp.com/go/dataprotector.

Техническая поддержка HP

Сведения о службах технической поддержки по всему миру см. на веб-сайте технической поддержки HP:

http://www.hp.com/support

Перед обращением в компанию HP соберите следующие сведения:

- названия и номера моделей продуктов;
- регистрационный номер для технической поддержки (если есть);
- серийные номера продуктов;
- сообщения об ошибках;
- тип и версию операционной системы;
- подробные вопросы.

Служба подписки

Компания HP рекомендует зарегистрировать продукт на веб-сайте службы Subscriber's Choice для бизнеса:

http://www.hp.com/go/e-updates

После регистрации на указанный адрес электронной почты будут приходить уведомления об улучшениях продукта, новых версиях драйверов, обновлениях встроенного ПО и других ресурсах продукта.

Веб-сайты HP

Дополнительные сведения см. на указанных ниже веб-сайтах компании HP.

- http://www.hp.com
- http://www.hp.com/go/dataprotector
- https://h20230.www2.hp.com/selfsolve/manuals
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Отзывы о документации

Компания HP ждет ваших отзывов.

Чтобы сделать замечания или внести предложения относительно документации по продукту, отправьте сообщение по адресу **DP.DocFeedback@hp.com**. Все отправленные сообщения становятся собственностью компании HP.

Глава 1. Обзор и необходимые компоненты

Обзор Data Protector for PCs

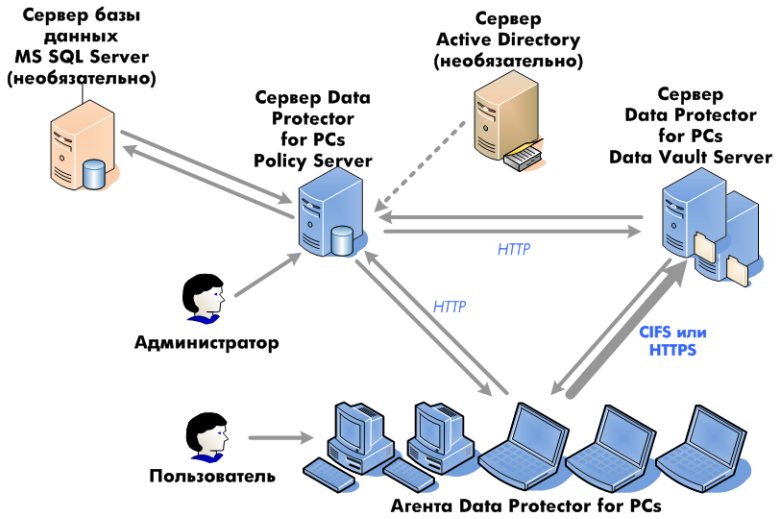
Система HP Data Protector for PCs состоит из двух основных программных компонентов — сервера Policy Server и агентов. Программное обеспечение Policy Server работает на сервере под управлением ОС Windows (поддерживаемые версии см. в матрице поддержки по адресу https://h20230.www2.hp.com/selfsolve/manuals). Агенты в фоновом режиме работают на всех настольных и переносных компьютерах.

Сервер Policy Server также может иметь доступ к группам и подразделениям на сервере Active Directory.

Для данных пользователей выполняется резервное копирование в хранилища Data Vault. Сервер Data Vault Server должен работать на отдельном компьютере, который не является сервером Policy Server. Если вместо рекомендуемых хранилищ Web Data Vault используются хранилища типа «общая папка Windows», они располагаются в одной или нескольких общих папках Windows на файловых серверах.

Архитектура Data Protector for PCs показана на приведенной ниже схеме.

Рисунок 1. Архитектура Data Protector for PCs



Для управления типами файлов, для которых выполняется резервное копирование с настольных и переносных компьютеров, а также местами хранения резервных копий используются различные политики. Они задаются в консоли Policy Server Console. Затем политики автоматически распространяются на агенты по протоколу SOAP через HTTP-порт 80. Политики хранятся на сервере Policy Server.

Агенты выполняют эти политики. Когда пользователь изменяет файл данных, защищенный в соответствии с политиками, на локальном жестком диске настольного или переносного

компьютера создается его предыдущая версия, а внесенные в файл изменения сжимаются и копируются во все применимые хранилища Data Vault.

При каждом резервном копировании файлов агент уведомляет сервер Policy Server, который содержит журнал аудита изменений файлов, внесенных пользователями. Помимо этого, каждый агент периодически отправляет на сервер Policy Server сведения о работоспособности. На основе этих данных в консоли Policy Server Console можно создавать отчеты.

Хранилища Data Vault находятся на сервере Data Vault Server. Клиентские данные копируются в хранилища Data Vault по двум разным протоколам: CIFS (для хранилищ Data Vault типа «общая папка Windows») или HTTP (для хранилищ Web Data Vault).

Сервер Data Vault Server должен работать на отдельном компьютере, который не является сервером Policy Server. Для использования протокола HTTPS на этом компьютере устанавливается программное обеспечение Web Data Vault Server и приложение Data Protector for PCs Cleanup. Для использования хранилищ Data Vault типа «общая папка Windows» на нем устанавливается только приложение Cleanup.

Если используется Active Directory, в Policy Server можно настроить доступ к группам и подразделениям. Тогда пользователям можно будет назначать хранилища Data Vault в зависимости от их членства в группе или подразделении. Кроме того, пользователей можно будет выбирать в отчетах на основе их членства.

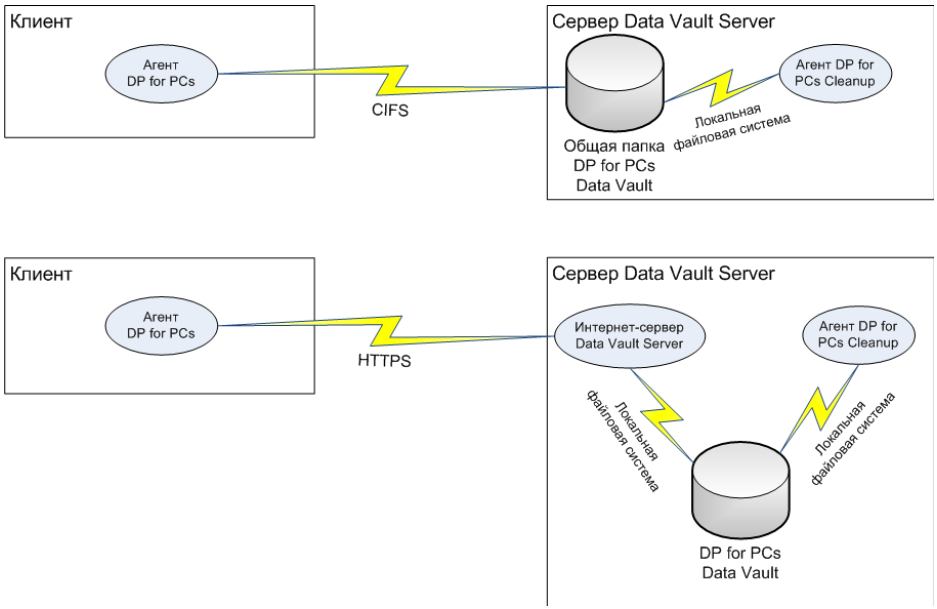
Хранилища Data Vault

В Data Protector for PCs поддерживается два типа хранилищ Data Vault.

- Хранилища Web Data Vault, доступ к которым осуществляется по протоколу HTTPS. Такие хранилища обеспечивают наивысший уровень безопасности и лучшую пропускную способность в средах с высокой задержкой, и поэтому рекомендуются к использованию.
- Хранилища Data Vault типа «общая папка Windows», доступ к которым осуществляется по протоколу CIFS. Такие хранилища использовались в более ранних версиях Data Protector for PCs.

Структура данных в хранилищах Data Vault обоих типов одинаковая, поэтому существующие хранилища Data Vault типа «общая папка Windows» можно преобразовать в хранилища Web Data Vault.

Рисунок 2. Сравнение хранилищ Data Vault типа «общая папка Windows» и Web Data Vault



Использование сертификата

Использование протокола SSL является обязательным условием для хранилищ Web Data Vault. Тип сертификата определяется во время установки хранилища Web Data Vault. Чтобы продукт был сразу готов к работе, например для пробного использования, можно установить сервер Web Data Vault Server с самозаверяющим сертификатом. Это не так безопасно, как использование сертификата, выпущенного доверенным центром сертификации. Чтобы обеспечить полную безопасность, для сервера Data Vault Server необходимо импортировать сертификат, подписанный центром сертификации, который считается доверенным в конкретной среде, и добавить его в серверный компонент.

Самозаверяющие сертификаты

При создании политики Data Vault Policy можно указать, допустимо ли использование самозаверяющих сертификатов. В этом случае на стороне агента не требуется выполнять какие-либо действия. Срок действия самозаверяющего сертификата, выпущенного при установке, составляет 20 лет.

Импортированные сертификаты

Процедура импорта предполагает наличие единственного файла в формате PEM, содержащего как закрытый ключ, так и соответствующий сертификат, включая открытый ключ. Учтите, что файл копируется в каталог конфигурации сервера Web Data Vault Server без изменений. В зависимости того, какая процедура использовалась для

создания файла сертификата, этот файл может быть зашифрован. В этом случае процесс службы Windows, отвечающий за работу сервера Web Data Vault Server, выдаст запрос на ввод пароля для расшифровки. Это произойдет во время установки и будет происходить при каждом перезапуске службы, например после перезагрузки компьютера. Чтобы запрос больше не выдавался, этот пароль можно вручную добавить в файл конфигурации Web Data Vault Server, однако процесс установки не поддерживает такую возможность. Если используется зашифрованный файл сертификата, пароль не рекомендуется хранить в файле рядом с ним.

ПРИМЕЧАНИЕ

Термин «доверенный центр сертификации» означает, что клиентские компьютеры, на которых запущен агент, будут считать этот центр сертификации надежным и принимать подписанные им сертификаты. Предполагается, что хранилища сертификатов Windows на клиентских компьютерах уже настроены соответствующим образом (сертификат центра и возможные дополнительные сертификаты добавлены в их цепочки). В агенте отсутствует какой-либо механизм для установки доверия. Для этого используются механизмы Windows.

Замена сертификата

После установки сервера Web Data Vault Server сертификат можно заменить в любое время с помощью программы DvConfig, описанной в разделе «Настройка параметров Web Data Vault из командной строки (DvConfig)»(стр. 21). Например, если при установке был выбран самозаверяющий сертификат, его можно заменить на импортированный.

Обзор установки Data Protector for PCs

ПРИМЕЧАНИЕ Если необходимо обновить установленное программное обеспечение Data Protector for PCs, см. «Обновление Data Protector for PCs»(стр. 43).

Установка Data Protector for PCs проходит в три этапа.

1. **Установка Data Protector for PCs Policy Server.**

   См. «Установка Data Protector for PCs Policy Server»(стр. 14).

2. **Установка ПО Data Protector for PCs Web Data Vault Server.**

   См. «Установка, настройка и обслуживание Web Data Vault Server»(стр. 18).

3. **Настройка политик защиты.**

   См. «Настройка политик защиты Data Protector for PCs»(стр. 23).

4. **Установка агентов Data Protector for PCs на переносных и настольных компьютерах.**

   См. «Установка агентов Data Protector for PCs»(стр. 38).

Необходимые компоненты

Policy Server

Поддерживаемые операционные системы см. в матрице поддержки.

ПРИМЕЧАНИЕ *Установка в 64-разрядной операционной системе Windows 2003.* В 64-разрядной операционной системе Windows сервер Policy Server работает в режиме совместимости с 32-разрядными приложениями. Это значит, что службы IIS должны работать в 32-разрядном режиме. Несоблюдение этого требования будет обнаружено мастером установки на этапе проверки необходимых компонентов. В этом случае пользователю будет предложено перевести службы IIS в 32-разрядный режим. Если на сервере имеются другие веб-приложения, для которых службы IIS должны работать в 64-разрядном режиме (например, Microsoft Exchange 2007 с веб-почтой Outlook Web Access), на нем нельзя будет установить Policy Server. Это примечание не относится к установке Policy Server в ОС Windows 2008.

На сервере должны быть установлены указанные ниже компоненты.

- Службы IIS 6.0, 7.0, 7.5 или более поздней версии с поддержкой приложений ASP.NET.

  В ОС Windows 2003 службы IIS 6.0 являются необходимым компонентом и должны быть установлены перед установкой Policy Server. В ОС Windows 2008 мастер установки Data Protector for PCs предложит установить службы IIS 7.0 и IIS 7.5, если они не установлены.

- Microsoft ASP.NET 2.0.

На сервере также должны быть установлены указанные ниже дополнительные компоненты.

- Установщик Microsoft версии 3.1 или более поздней (требуется для .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 или более поздней версии. Мастер установит версию 2.0 SP1.
- Microsoft SQL Express (если другие версии SQL отсутствуют).

Кроме того, только для служб IIS 7.0 и IIS 7.5 требуются указанные ниже компоненты IIS. Если они отсутствуют, мастер предложит их установить.

- Веб-сервер статического содержимого IIS — для обслуживания статических HTML-файлов, документов и изображений.
- IIS ASP.NET — для развертывания ASP.NET 2.0 и .NET Framework.
- Безопасность IIS — для встроенной проверки подлинности Windows, используемой консолью Policy Server Console.
- Совместимость управления IIS 6 — для одинаковой настройки служб IIS 6 и IIS 7 с помощью программы установки, насколько это возможно.

База данных

Системе Data Protector for PCs требуется доступ к базе данных Microsoft SQL Server. Поддерживаемые версии см. в матрице поддержки.

Чтобы проверить (или изменить) режим проверки подлинности SQL Server, можно воспользоваться Microsoft Enterprise Manager.

1. Щелкните правой кнопкой мыши экземпляр SQL Server, выберите пункт **Свойства** и откройте вкладку **Безопасность**.
2. Должен быть установлен переключатель **SQL Server и Windows** (а не **Только Windows**). Если это не так, установите его и нажмите кнопку **OK**.

Можно также установить экземпляр Microsoft SQL Server Express Edition во время установки Data Protector for PCs.

Data Protector for PCs Web Data Vault Server

- Сервер Web Data Vault Server должен быть установлен на отдельном компьютере, который не является сервером Policy Server. (Его можно установить на том же компьютере, но такой вариант подходит только для пробного использования.)
- Должна быть установлена среда выполнения Java Runtime Environment версии 1.6 или более поздней.
- Переменные JAVA_HOME и JRE_HOME должны указывать на каталог установки Java Runtime.

Агенты Data Protector for PCs

Программное обеспечение агента Data Protector for PCs может быть установлено на настольных и переносных компьютерах пользователей, работающих под управлением ОС Windows. Поддерживаемые платформы см. в матрице поддержки.

Глава 2. Установка Data Protector for PCs Policy Server

ПРИМЕЧАНИЕ Чтобы обновить версию уже установленного программного обеспечения Data Protector for PCs Policy Server, нужно следовать стандартной процедуре установки. Дополнительные сведения см. в разделе «Обновление Policy Server»(стр. 43).

Быстрая установка

Требования для Data Protector for PCs Policy Server см. в разделе «Policy Server»(стр. 12).

1. Вставьте установочный компакт-диск Data Protector for PCs. Если мастер установки не запустился автоматически, запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Следуйте инструкциям на экране.
3. Программному обеспечению Data Protector for PCs Policy Server требуется доступ к базе данных Microsoft SQL Server. Установите переключатель **Установить экземпляр Data Protector for PCs сервера Microsoft SQL Server Express** или **Использовать существующий экземпляр Microsoft SQL Server** . Если выбрано использование существующего экземпляра SQL Server, необходимо указать строку подключения к серверу базы данных и учетные данные учетной записи, у которой достаточно прав для создания новой базы данных.
4. Нажмите кнопку **Установить** на странице мастера **Установка Data Protector for PCs Policy Server**, чтобы начать установку.
5. После завершения установки нажмите кнопку **Далее**. Затем можно запустить консоль Data Protector for PCs Policy Server Console.
6. Установите на отдельном компьютере сервер Web Data Vault Server. В главном меню установки выберите пункт **Установка Data Vault**.

ПРИМЕЧАНИЕ В ходе установки приложение Cleanup всегда устанавливается вместе с ПО Web Data Vault Server. Если на сервере Data Vault Server находятся только хранилища Data Vault типа «общая папка Windows», это приложение рекомендуется установить локально для оптимизации производительности.

Подробная установка

ПРИМЕЧАНИЕ

Только для ОС Windows 2003 Server. Программное обеспечение Data Protector for PCs Policy Server можно установить с компакт-диска с общим доступом по сети или из сетевой общей папки, только если на сервере для зоны безопасности локальной интрасети используется политика безопасности среды выполнения .NET Framework 2.0 *Полное доверие*, . Если на сервере отсутствует локальное устройство чтения компакт-дисков, измените политику безопасности среды выполнения для зоны безопасности локальной интрасети на *Полное доверие*, используя средство настройки .NET Framework 2.0 из раздела «Администрирование», или скопируйте папку Server с компакт-диска на локальный диск сервера.

Для установки Data Protector for PCs Policy Server в систему необходимо войти с учетной записью, обладающей правами администратора.

1. Вставьте установочный компакт-диск Data Protector for PCs. Если мастер установки не запустился автоматически, запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Выберите пункт **Установка Policy Server**.

   При запросе выберите вариант **Открыть** (или **Запустить**) эту программу из текущего места, а не **Сохранить эту программу на диске**.
3. Для работы Data Protector for PCs Policy Server требуется платформа .NET Framework 2.0 SP1. Если она еще не установлена, появится запрос на установку с компакт-диска.

   Для установки требуется установщик Windows версии 3.1 или более поздней, поэтому при необходимости появится запрос на его установку с компакт-диска.
4. Мастер установки проверит наличие остальных необходимых компонентов:
   - служб IIS;
   - ASP.NET 2.0.

   Если какой-либо из этих компонентов отсутствует, щелкните его в списке, чтобы получить сведения об установке.

   Нажмите кнопку **Далее**.
5. Установите Microsoft SQL Server.

   Использование существующего экземпляра Microsoft SQL Server

a. Установите переключатель **Использовать существующий экземпляр Microsoft SQL Server**.

b. В поле **Сервер базы данных** введите строку подключения к существующему серверу базы данных.

c. В полях **Имя для входа** и **Пароль** введите учетные данные учетной записи, у которой достаточно прав для создания новой базы данных. Обычно используется учетная запись «sa».

d. Нажмите кнопку **Далее**. Указанные параметры подключения будут использованы для проверки подключения к существующему серверу базы данных. При успешном подключении мастер перейдет к шагу 6.

Установка экземпляра Data Protector for PCs сервера Microsoft SQL Server Express Edition

a. Установите переключатель **Установить экземпляр DataProtectorNE сервера Microsoft SQL Server Express** и нажмите кнопку **Далее**.

b. Нажмите кнопку **Установить**, чтобы установить экземпляр Microsoft SQL Server 2005 Express Edition с именем «DataProtectorNE». После завершения установки нажмите кнопку **Далее**.

6. Установите программное обеспечение Data Protector for PCs Policy Server.

a. На странице приветствия нажмите кнопку **Далее**, чтобы начать установку.

- Консоль Data Protector for PCs Policy Server Console будет установлена как веб-приложение в виртуальном каталоге C:\Inetpub\wwwroot\dpnepolicy.
- Веб-служба Data Protector for PCs будет установлена в каталоге C:\Inetpub\wwwroot\dpnepolicyservice.

Оба компонента используют протокол HTTP (порт 80).

b. После завершения установки Policy Server нажмите кнопки **Закрыть** и **Далее**.

7. Установите приложение Cleanup. Нажмите кнопку **Установить**, чтобы начать установку.
8. После завершения установки Cleanup нажмите кнопку **Далее**.

Администрирование Data Protector for PCs выполняется централизованно из консоли Data Protector for PCs Policy Server Console. Поскольку консоль является веб-приложением, для управления Data Protector for PCs можно использовать любой компьютер с возможностью подключения браузера к Policy Server (через HTTP-порт 80).

Чтобы запустить консоль Data Protector for PCs Policy Server Console в браузере на сервере Policy Server, не снимайте флажок **Запустить Policy Server Console** и нажмите кнопку **Готово**.

ПРИМЕЧАНИЕ Во время установки приложение Cleanup устанавливается на сервере Policy Server. Для оптимизации производительности его также рекомендуется установить на компьютерах с хранилищами Data Vault.

ПРИМЕЧАНИЕ

Параметры браузера для консоли Policy Server Console. Если при отображении страниц консоли Policy Server Console в браузере возникли проблемы, проверьте параметры безопасности браузера. Для правильной работы консоли выполните указанные ниже действия.

- Включите JavaScript.
- Отключите блокирование всплывающих окон для веб-сайта dpnepolicy.
- При необходимости измените другие параметры ограничений безопасности в зависимости от конкретного браузера и его версии.

Установка на сервере с Microsoft SharePoint. Если программное обеспечение Policy Server установлено на сервере с Microsoft SharePoint, при запуске консоли Policy Server Console может появиться сообщение об ошибке 404 «Невозможно найти страницу». Эта проблема и ее решение описаны в статье базы знаний Microsoft по адресу http://support.microsoft.com/kb/828810. Обратите внимание, что такая проблема характерна для всех веб-приложений ASP.NET, а не только для Policy Server.

Чтобы ПО Policy Server работало на сервере с SharePoint, выполните указанные ниже действия.

1. С помощью средств администрирования SharePoint создайте исключения для двух веб-приложений Policy Server — dpnepolicy и dpnepolicyservice.
2. Измените для Policy Server два файла web.config (dpnepolicy\web.config и dpnepolicyservice\web.config), добавив в них XML-код <httpHandlers> и <trust>, как описано в указанной выше статье базы знаний Microsoft.

Глава 3. Установка, настройка и обслуживание Web Data Vault Server

Установка и настройка Web Data Vault Server

ПРИМЕЧАНИЕ Сервер Web Data Vault Server должен быть установлен на отдельном компьютере, который не является сервером Policy Server. (Его можно установить на том же компьютере, но такой вариант подходит только для пробного использования.)

1. Вставьте установочный компакт-диск Data Protector for PCs. Если мастер установки не запустился автоматически, запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Выберите пункт **Установка Data Vault**.
3. Выберите один из вариантов установки.
   - **Web Data Vault Server** (рекомендуется). Этот вариант также предусматривает установку на сервере приложения Cleanup.
   - **Приложение Cleanup для Data Vault типа «общая папка Windows»**. Выберите этот вариант, если предполагается использовать только хранилища Data Vault типа «общая папка Windows».

   Дополнительные сведения см. в разделе «Хранилища Data Vault»(стр. 9).
4. Следуйте инструкциям на экране до завершения этапа установки.
5. При установке Web Data Vault Server после получения лицензии с сервера Policy Server начинается настройка хранилища Web Data Vault.

   На странице «Параметры сервера» введите полное доменное имя и SSL-порт сервера. То же самое полное доменное имя нужно будет использовать при настройке политики Data Vault на сервере Policy Server. Это имя должно быть разрешимым на всех клиентских компьютерах; в противном случае для некоторых из них будет невозможно выполнить резервное копирование данных в хранилища Data Vault на этом сервере.
6. На странице «Параметры сертификата» нужно выбрать один из вариантов.
   - Импорт существующего SSL-сертификата, выпущенного доверенным центром сертификации (ЦС). Это рекомендуемый вариант, который обеспечивает наивысший уровень безопасности.
   - Создание самозаверяющего SSL-сертификата. Этот вариант менее безопасный и должен использоваться только для пробного использования.

ПРИМЕЧАНИЕ После установки сертификат на сервере Web Data Vault Server можно заменить в любое время с помощью программы DvConfig. Например, если при установке был выбран самозаверяющий сертификат, его можно заменить на импортированный. См. раздел «Настройка параметров Web Data Vault из командной строки (DvConfig)»(стр. 21).

7. На следующей странице необходимо указать имена для двух типов пользователей сервера Web Data Vault Server.
   - **Администратор** — пользователь, который выполняет административные задачи, такие как создание и удаление хранилищ Data Vault, а также миграция клиентских данных резервного копирования.
   - **Пользователь, выполняющий резервное копирование** — пользователь, который выполняет пользовательские операции, такие как резервное копирование и восстановление файлов.

   Это пользователи сервера Data Protector for PCs Web Data Vault Server. Учетные данные обоих пользователей необходимо будет вводить при создании и изменении хранилищ Web Data Vault на этом сервере.

   ПРИМЕЧАНИЕ Пароли должны быть не короче 8 символов.

8. Нажмите кнопку **Далее**, а затем — **Готово**, чтобы завершить установку и настройку сервера Web Data Vault Server, а также установку приложения Cleanup.

Обслуживание хранилищ Web Data Vault

1. На странице политики Data Vault укажите полное доменное имя и SSL-порт сервера, а также учетные данные пользователя, выполняющего резервное копирование. Затем нажмите кнопку **Настройка Data Vault**.
2. Отправьте учетные данные администратора, после чего откроется страница обслуживания Web Data Vault Server.

   Здесь можно выбрать или удалить существующие хранилища Web Data Vault. Можно также добавить новое хранилище Data Vault.

   ПРИМЕЧАНИЕ Существующее хранилище Data Vault можно выбрать, только если оно в данный момент не подключено к другой политике Data Vault.

3. Сохраните политику Data Vault, нажав кнопку **Сохранить** в нижней части страницы.
4. Если было добавлено новое хранилище Data Vault, при необходимости можно проверить его существование и правильность настройки.

Миграция данных из хранилища Data Vault типа «общая папка Windows» в хранилище Web Data Vault

Структура данных в Data Vault не зависит от типа хранилища, будь то общая папка Windows или Web Data Vault с доступом по протоколу HTTPS. Это значит, что данные из существующих хранилищ Data Vault версии DPNE 6.x можно перенести в новые хранилища Web Data Vault.

ПРИМЕЧАНИЕ Миграцию данных можно выполнить только для тех хранилищ Data Vault, которые относятся к одному серверу Policy Server или имеют одинаковый пароль шифрования.

Существует два возможных сценария миграции данных.

- Размещение хранилища Web Data Vault на том же компьютере.

  ПРИМЕЧАНИЕ Одновременное обращение к одному каталогу как к общей папке Windows и как к Web Data Vault не поддерживается.

- Перенос всего хранилища Data Vault на другой компьютер.

В обоих случаях сервер Web Data Vault Server должен быть установлен локально на компьютере, на котором будут храниться данные.

Миграция данных из существующего хранилища Data Vault типа «общая папка Windows» в хранилище Web Data Vault

ПРИМЕЧАНИЕ

- Миграцию следует выполнять в нерабочее время, чтобы минимизировать последствия для выполняющихся операций резервного копирования.
- Откройте диспетчер задач Windows и убедитесь, что программа DPNECleanup.exe не запущена.
- Откройте политику Cleanup на сервере Policy Server и убедитесь, что запуск программы DPNECLeanup.exe не запланирован на период миграции.

1. Установите сервер Web Data Vault Server и обновите сервер Policy Server и агенты до версии 7.0. Убедитесь, что после установки версии 7.0 все агенты были перезагружены, так как только после этого они смогут выполнять резервное копирование данных в хранилище Web Data Vault.
2. Отключите соответствующую политику для общей папки Windows на странице политики Data Vault, чтобы агенты перестали копировать данные в Data Vault.
3. Если для хранилища Web Data Vault предполагается использовать тот же каталог, прекратите общий доступ к этому каталогу по протоколу CIFS.
4. Если хранилище Web Data Vault и общая папка Windows находятся на разных серверах, данные необходимо скопировать на компьютер Web Data Vault в папку, длина пути к которой не превышает 67 символов. Если хранилище Data

Vault находится на том же сервере, данные не нужно копировать в новое место, если на то нет особых причин.

5. Перед созданием нового хранилища Web Data Vault продумайте процесс начального обновления. Начальное обновление можно пропустить, если его уже выполнили все агенты и существующее хранилище Data Vault содержит все данные резервного копирования. В самой политике Data Vault отсутствует параметр, позволяющий пропустить начальное обновление, однако он есть в политике копирования, на которую та ссылается. Убедитесь в существовании политики Data Vault с правильно выбранными параметрами (с отключенным начальным обновлением и подходящими параметрами регулирования и расписания). Для этого можно создать новую политику копирования или изменить существующую (в этом случае будут затронуты все политики Data Vault, которые ссылаются на эту политику копирования).
6. Создайте и сохраните новую политику Data Vault для хранилища Web Data Vault. При создании нового хранилища Web Data Vault необходимо указать путь к папке. В данном случае это будет путь к общей папке Windows с данными существующего хранилища Data Vault, которые необходимо перенести. Выберите политику копирования, созданную на шаге 5. Задайте остальные параметры политики Data Vault такими же, как и в исходной политике Data Vault для общей папки Windows (например, параметры сети, параметры Active Directory).
7. Убедитесь, что агенты успешно копируют файлы в новое хранилище Web Data Vault, после чего удалите исходную политику Data Vault для общей папки Windows.

После сохранения политики агенты возобновят копирование данных в новое хранилище Web Data Vault по протоколу HTTPS.

Настройка параметров Web Data Vault из командной строки (DvConfig)

С помощью этой программы командной строки можно изменить параметры конфигурации Web Data Vault, такие как имя и пароль пользователя, выполняющего резервное копирование, и администратора, импортировать новый сертификат, изменить SSL-порт и создать новый самозаверяющий сертификат.

Прежде чем изменять какие-либо параметры, необходимо остановить сервер Web Data Vault Server, остановив службу Windows с именем HP Data Protector for PCs Data Vault Server.

После внесения изменений следует перезапустить службу Web Data Vault. Все обновленные политики будут повторно распространены на агенты.

ПРИМЕЧАНИЕ Если программа DvConfig используется для изменения SSL-порта либо имени или пароля пользователя, выполняющего резервное копирование, на сервере Web Data Vault Server, внесите необходимые изменения в соответствующие политики Data Vault на сервере Policy Server.

Использование

DvConfig [-adminUser *имя_для_входа*:*пароль* -backupUser *имя_для_входа*:*пароль*] [-h] [-i *файл_сертификата* | -s *имя_узла*] [-p *порт*] [-v]

-adminUser *имя_для_входа*:*пароль*

Задание учетных данных для учетной записи DvAdmin. Если не указано имя для входа или пароль, используется значение по умолчанию «DvAdmin».

-backupUser *имя_для_входа*:*пароль*

Задание учетных данных для учетной записи DvBackup. Если не указано имя для входа или пароль, используется значение по умолчанию «DvBackup».

–h

Вывод этого сообщения.

-i *файл_сертификата*

Импорт существующего сертификата.

-p *порт*

Задание SSL-порта

–s *имя_узла*

Создание самозаверяющего сертификата для полного доменного имени.

–v

Вывод сведений о версии и выход.

Глава 4. Настройка политик защиты Data Protector for PCs

Начальная настройка после установки Data Protector for PCs

Сразу после установки Data Protector for PCs в консоли Policy Server Console отображается окно начальной настройки. Она выполняется перед настройкой политик Data Protector for PCs и проходит в два этапа.

1. **Задание или импорт пароля шифрования.**

   По соображениям безопасности перед использованием Data Protector for PCs следует задать пароль шифрования. Это обеспечит шифрование всех файлов на компьютере пользователя и их передачу по сети в зашифрованном виде. Один пароль используется для всех пользователей и всех централизованных хранилищ Data Vault.

   - Для централизованного хранилища Data Vault (заданного в консоли Policy Server Console) всегда используется шифрование на основе пароля Data Protector for PCs.
   - Для локальных хранилищ Data Vault (заданных пользователями на своих компьютерах) каждый пользователь может самостоятельно решить, нужно ли использовать шифрование, и выбрать собственный пароль.

   При первой установке Data Protector for PCs, прежде чем продолжить, необходимо **создать** или **импортировать** пароль. В целях безопасности после создания пароль необходимо **экспортировать**. Таким образом он будет сохранен в безопасном месте. В дальнейшем его можно будет использовать для импорта.

   Для управления паролем щелкните ссылку **Задать политику шифрования** и следуйте инструкциям на экране.

   ПРИМЕЧАНИЕ После создания или импорта пароль нельзя изменить.

2. **Лицензирование Data Protector for PCs.**

   Ознакомительная версия Data Protector for PCs работает в течение 60 дней и обеспечивает защиту неограниченного количества пользователей без последующего лицензирования. После приобретения Data Protector for PCs необходимо зайти на страницу службы выдачи лицензионных ключей HP License Key Delivery Service по адресу https://webware.hp.com/welcome.asp и загрузить ключ лицензии для последующего ввода. Для приобретения доступны следующие лицензии:

   - TA032AA или TA032AAE на 100 агентов;
   - TA033AA или TA033AAE на 1000 агентов;

- TA036AA или TA036AAE на 100 агентов вместе с HP Data Protector Starter Pack для Windows (B6961BA или B6961BAE).

Ключ постоянной лицензии нужно ввести до окончания периода пробного использования. В противном случае через 60 дней агенты больше не смогут копировать данные в свои репозитории Local Repository или хранилища Data Vault. При этом возможность восстановления ранее защищенных версий файлов сохранится.

Для управления лицензиями выберите пункт **Управление лицензиями** и щелкните ссылку **Ввести ключ лицензии для пользователей Data Protector for PCs**. Следуйте инструкциям на экране.

ПРИМЕЧАНИЕ Лицензии распространяются на агенты при их установке.

После успешного выполнения этих действий становится доступна полнофункциональная версия консоли Policy Server. В следующем разделе описан порядок настройки остальных элементов Data Protector for PCs сразу после установки Data Protector for PCs.

Первичная настройка

Программное обеспечение Data Protector for PCs поставляется с настроенными политиками, которые подойдут большинству организаций. Рекомендуется сначала настроить политики Data Vault, копирования и защиты файлов, а затем установить агент Data Protector for PCs на настольных и переносных компьютерах пользователей.

ПРИМЕЧАНИЕ Можно не создавать новые политики, а изменить уже настроенные, поставляемые с Data Protector for PCs. Для этого на каждом этапе вместо ссылки **Создать новую политику** нужно щелкать ссылку **Изменить существующую политику**.

Политики защиты для установленного программного обеспечения настраиваются в консоли Policy Server Console. Централизованные политики распространяются на все агенты Data Protector for PCs и выполняются на настольных и переносных компьютерах пользователей.

1. Запустите консоль Data Protector for PCs Policy Server Console в конце установки или в любое другое время, указав в браузере следующий URL-адрес:

   http://*policyserver*/dpnepolicy/

   где «*policyserver*» — имя сервера Data Protector for PCs Policy Server. Для этого необходимо войти на сервер как администратор.

2. **Настройка политик Data Vault**.

   Политики Data Vault задают место назначения (хранилище Web Data Vault или общую папку Windows) для постоянного резервного копирования пользовательских файлов, защищенных политиками. Когда в файл вносятся изменения, предыдущую версию и измененный файл можно автоматически архивировать в одно или

несколько мест назначения. Каждой группе пользователей можно назначить одно или несколько хранилищ Data Vault. Например, можно задать политику Data Vault с именем *Продажи* и назначить ее группам пользователей *Продажи.Липецк*, *Продажи.Самара*, *Продажи.Чита* и *Продажи.Астрахань*.

- Для централизованного хранилища Data Vault (заданного в консоли Policy Server Console) всегда используется шифрование на основе пароля Data Protector for PCs.
- Для локальных хранилищ Data Vault (заданных пользователями в программном обеспечении агента) каждый пользователь может самостоятельно решить, нужно ли использовать шифрование, и выбрать собственный пароль.

ПРИМЕЧАНИЕ *Требование для всех хранилищ Data Vault*

Программное обеспечение Data Protector for PCs установит такие же разрешения на доступ (ACL) к резервным копиям файлов на файловом сервере, как и у исходных файлов. Это значит, что пользователи смогут восстанавливать файлы из резервных копий только в том случае, если у них есть доступ к исходным файлам на компьютере.

Требование для хранилищ Data Vault типа «общая папка Windows»

При использовании стандартных хранилищ Data Vault типа «общая папка Windows» общие папки должны находиться на файловом сервере Windows, который не является сервером Policy Server. Вместе с тем, на время пробного использования Data Protector for PCs с небольшим количеством установленных агентов может быть удобно разместить сервер Policy Server и файловый сервер Data Vault на одном компьютере.

Создание политики Data Vault

a. В области навигации слева выберите пункты **Политики > Хранилища Data Vault > Политики Data Vault**.

b. Щелкните ссылку **Создать новую политику Data Vault**.

c. Следуйте инструкциям на экране. Процедура зависит от выбранного типа Data Vault («Web Data Vault» или «Общая папка Windows»).

ПРИМЕЧАНИЕ При создании Data Vault длина пути к папке (или общей папке) не должна превышать 66 символов.

Рекомендации

На данный момент оставьте политику копирования по умолчанию.

Рекомендации для приложения Cleanup, используемого для хранилищ Data Vault типа «общая папка Windows»

- Если хранилище Data Vault находится на этом сервере Policy Server, оставьте параметр имени этого компьютера по умолчанию.

- Если хранилище Data Vault находится на другом файловом сервере Windows, установите на нем приложение Data Vault Cleanup и назначьте его как компьютер Cleanup.

3. **Настройка политик копирования**.

   Политика копирования задает ограничение по числу клиентов, которые могут одновременно копировать данные в Data Vault. Она также определяет параметры начального и запланированного обновления Data Vault в дополнение к постоянному резервному копированию. Каждая политика копирования может быть назначена одному или нескольким хранилищам Data Vault.

   Политики копирования определяют указанные ниже параметры.

   - Число агентов, которые могут одновременно копировать файлы в хранилища Data Vault.
   - Расписание периодических обновлений, которое обеспечивает проверку наличия всех предполагаемых файлов пользователей в Data Vault и копирование отсутствующих файлов. Это дополнительно гарантирует правильность копирования всех файлов пользователей в Data Vault.
   - Необходимость выполнения **начального обновления** (или копирования). Начальное обновление является необходимым, так как при нормальной работе Data Protector for PCs каждый раз, когда пользователь изменяет файл, который находится под постоянной защитой Data Protector for PCs, в Data Vault копируются только сведения об изменениях.

   Политика копирования по умолчанию применяется ко всем хранилищам Data Vault, для которых не задана отдельная политика. В политике по умолчанию можно изменить параметры, но ее нельзя удалить или переименовать.

   Создание политики копирования

   a. В области навигации слева выберите пункт **Политики**.

   b. Щелкните ссылку **Задать политики копирования**.

   c. Щелкните ссылку **Создать новую политику копирования**.

   d. Следуйте инструкциям на экране.

   Рекомендации

   - **Регулирование**. Задайте период, соответствующий обычному рабочему времени, и укажите нижний предел регулирования для остального времени.
   - **Начальное обновление**. Включите начальное обновление, чтобы обеспечить резервное копирование всех пользовательских файлов, защищенных с помощью политик защиты файлов.
   - **Обновлять файлы каждую неделю/месяц**. Поскольку обновление должно содержать несколько копий файлов, если таковые имеются, включите обновления Data Vault, чтобы обеспечить правильное резервное копирование всех пользовательских файлов, защищенных с помощью политик.

4. **Настройка политик защиты файлов**.

Политики защиты файлов позволяют указать типы файлов для защиты и срок хранения предыдущих версий. Например, для документов Word, электронных таблиц Excel и презентаций PowerPoint можно задать политику защиты файлов с именем *Документы Office*.

Файлы, хранящиеся на локальных дисках, можно защитить.

Существует два типа политик.

- **Continuous File Protection**. Такие политики обеспечивают защиту файлов в режиме реального времени в момент их сохранения на диск или удаления. Как правило, любой файл или документ, в меню которого имеется пункт **Сохранить**, должен быть защищен с помощью политики Continuous File Protection.

  Программное обеспечение Data Protector for PCs содержит различные примеры политик. Три из них выбраны по умолчанию после установки: *Документы Office*, *Разработка ПО* и *Веб-документы*. Можно начать с использования этих политик или создать собственные.

- **Open File Protection**. Такие политики обеспечивает защиту файлов путем периодического (обычно один раз в час) создания «снимка» файла С помощью данного метода обычно защищаются файлы, которые имеют очень большой размер (больше 100 МБ), открыты большую часть времени либо для которых отсутствует пункт меню **Сохранить**. Распространенными файлами этого типа являются файлы электронной почты и баз данных.

  Программное обеспечение Data Protector for PCs содержит четыре примера: *Microsoft Outlook*, *Microsoft Outlook Express*, *Почта Windows* и *Thunderbird*. Можно начать с использования этих политик или создать собственные.

  ПРИМЕЧАНИЕ Программное обеспечение Data Protector for PCs не поддерживает резервное копирование файлов, зашифрованных с помощью EFS, с использованием политик Open File Protection, поэтому такие файлы, как PST, не должны быть зашифрованы с помощью EFS.

Создание политики защиты файлов

a. В области навигации слева выберите пункт **Политики**.

b. Щелкните ссылку **Задать политики защиты файлов**.

c. Щелкните ссылку **Создать новую политику Continuous File Protection** или **Создать новую политику Open File Protection**.

d. Следуйте инструкциям на экране.

ПРИМЕЧАНИЕ При создании политик защиты файлов и настройке правил исключения или включения длина расширений файлов не должна превышать 9 символов для политик Open File Protection и 29 символов для политик Continuous File Protection.

Для политик Open File Protection в правилах включения можно выбирать файлы без расширения. Политики Continuous File Protection не поддерживают такую возможность.

ВАЖНО На данном этапе настроены все основные политики, необходимые для работы Data Protector for PCs. Остальные политики Data Protector for PCs настроены разработчиком и подойдут большинству организаций. Рекомендуется сразу приступить к установке агентов на настольные и переносные компьютеры пользователей (см. «Установка агентов Data Protector for PCs»(стр. 38)). В дальнейшем можно будет вернуться к просмотру и настройке остальных политик Data Protector for PCs, таких как политика Cleanup, политика управления пользователями, политика обновления агента и политика хранения данных отчетности.

Настройка остальных политик

1. **Настройка доступа к Active Directory**.

ПРИМЕЧАНИЕ *Сопоставление групп Active Directory с хранилищами Data Vault.* Хранилища Data Vault можно сопоставить с группами Active Directory в политике Data Vault. Данные всех членов сопоставленных групп будут архивироваться в сопоставленное хранилище Data Vault. Отдельных пользователей сопоставлять нельзя. Более того, если сопоставить подразделение, будут сопоставлены только группы из этого подразделения. Пользователи, которые находятся непосредственно в подразделении, не будут сопоставлены с Data Vault. Список групп Active Directory может ошибочно содержать не только группы безопасности, но и другие группы, например группы рассылки. Однако в действительности с Data Vault будут сопоставлены только группы безопасности.

Несколько пользователей. Если на одном компьютере работают несколько пользователей, они должны входить в одну группу Active Directory.

Чтобы назначать хранилища Data Vault или создавать отчеты по группам или подразделениям, в Policy Server необходимо настроить доступ к Active Directory.

После настройки доступа к Active Directory для хранилищ Data Vault становится доступен параметр **Члены групп и организационных подразделений** (см. раздел «Первичная настройка»(стр. 24)).

Настройка доступа к Active Directory

a. В области навигации слева выберите пункт **Конфигурация**.

b. Щелкните ссылку **Настройка доступа к Active Directory**.

c. Следуйте инструкциям на экране.

2. Настройка политики Cleanup.

Локальные репозитории Data Protector for PCs Local Repository на компьютерах пользователей и хранилища Data Vault на серверах Data Vault Server нуждаются в периодической очистке для удаления версий, у которых истек срок хранения, указанный в параметрах политик защиты файлов.

Настройка политики Cleanup

a. В области навигации слева выберите пункт **Политики**.

b. Щелкните ссылку **Задать политику Cleanup**.

c. Следуйте инструкциям на экране.

Если необходимо обеспечить поддержку хранилищем Data Vault большего количества пользователей, запускайте процесс очистки только по выходным, начиная с вечера пятницы или раннего утра субботы, чтобы на ее выполнение осталось как можно больше времени.

a. Откройте в консоли администратора Policy Server страницу политики Cleanup и измените параметры в разделе **Расписание Data Vault Cleanup**.

b. Снимите флажки напротив всех дней, кроме пятницы или субботы.

- Для пятницы выберите время запуска вечером, например в 22:00.
- Для субботы выберите время запуска ранним утром, например в 1:00.

Особенности очистки только по выходным

- Список файлов, доступных для восстановления из Data Vault, до конца недели устареет. Чтобы получить актуальное представление, пользователи в любой момент могут вручную запустить повторную проверку своих данных в Data Vault.
- Устаревшие резервные копии будут существовать до конца недели, так как очистка выполняется только по выходным.
- Управление квотами будет несвоевременным. Если пользователи превысят свои квоты, они должны будут дождаться очистки, чтобы снова получить свободное место в Data Vault. С другой стороны, превышение квоты будет распознаваться не сразу, так как данные об использовании дискового пространства передаются в процессе очистки.

Рекомендации

- **Расписание Local Repository Cleanup**. Оставьте значение по умолчанию «1 час».
- **Расписание Data Vault Cleanup**. Параметры по умолчанию, предусматривающие ежедневную очистку в полночь, должны подойти для большинства установленных приложений. Дополнительные сведения об

объеме Data Vault см. в разделе «Рекомендации по масштабированию»(стр. 32).

- Чтобы оптимизировать использование процессора и дискового пространства, программу DPNECleanup можно настроить для работы в многопоточном режиме с возможностью повторного использования потоков и расширения. Это позволит хранить больший объем данных. См. «Настройка многопоточного режима Cleanup»(стр. 35).

3. **Настройка политики управления пользователями**.

   Политика управления пользователями определяет полномочия пользователей в отношении корпоративных политик, распространенных на их компьютеры.

   Настройка политики управления пользователями

   a. В области навигации слева выберите пункт **Политики**.

   b. Щелкните ссылку **Задать политику управления пользователями**.

   c. Следуйте инструкциям на экране.

   Рекомендации

   Установите переключатель в столбце **Разрешить управление пользователями** для политики **Самостоятельное восстановление**.

4. **Настройка политики обновления агента**.

   Эта политика назначает версию агента Data Protector for PCs, которая должна использоваться на всех настольных и переносных компьютерах, защищенных с помощью Data Protector for PCs и автоматически обновляемых до этой версии.

   Настройка политики обновления агента

   a. В области навигации слева выберите пункт **Политики**.

   b. Щелкните ссылку **Задать политику обновления агента**.

   c. Следуйте инструкциям на экране.

5. **Настройка хранения данных отчетности**.

   Эти параметры определяют срок, в течение которого данные хранятся для отчетности по каждой из основных категорий информации.

   Настройка хранения данных отчетности

   a. В области навигации слева выберите пункт **Конфигурация**.

   b. Щелкните ссылку **Настройка хранения данных отчетности**.

   c. Следуйте инструкциям на экране.

Другие задачи настройки

Эти задачи обычно выполняются при первой установке Data Protector for PCs.

Лицензирование программного обеспечения Data Protector for PCs

Ознакомительная версия Data Protector for PCs работает в течение 60 дней и обеспечивает защиту неограниченного количества пользователей без последующего лицензирования. После приобретения Data Protector for PCs необходимо зайти на страницу службы выдачи лицензионных ключей HP License Key Delivery Service по адресу https://webware.hp.com/welcome.asp и загрузить ключ лицензии для последующего ввода.

Ввод ключа лицензии

1. В области навигации слева выберите пункт **Управление лицензиями**.
2. Щелкните ссылку **Ввести ключ лицензии для пользователей HP Data Protector for PCs**.
3. Следуйте инструкциям на экране.

Если необходимо указать несколько лицензий, можно создать текстовый файл, содержащий по ключу в каждой строке. Затем этот файл можно будет импортировать с помощью поля «Импортировать ключ(и) лицензии».

ПРИМЕЧАНИЕ Лицензии распространяются на агенты при их установке.

Перенос лицензий

Если необходимо изменить IP-адрес Policy Server, чтобы перенести сервер на другой компьютер, или перенести лицензии с одного сервера Policy Server на другой, обратитесь в службу выдачи лицензионных ключей HP License Key Delivery Service по адресу https://webware.hp.com/welcome.asp.

Задание, импорт и экспорт пароля шифрования

По соображениям безопасности перед использованием Data Protector for PCs следует задать пароль шифрования. Это обеспечит шифрование всех файлов на компьютере пользователя и их передачу по сети в зашифрованном виде. Один пароль используется для всех пользователей и всех централизованных хранилищ Data Vault.

- Для централизованного хранилища Data Vault (заданного в консоли Policy Server Console) всегда используется шифрование на основе пароля Data Protector for PCs.
- Для локальных хранилищ Data Vault (заданных пользователями на своих компьютерах) каждый пользователь может самостоятельно решить, нужно ли использовать шифрование, и выбрать собственный пароль.

При первой установке Data Protector for PCs, прежде чем продолжить, необходимо создать или импортировать пароль. В целях безопасности после создания пароль необходимо экспортировать. Таким образом он будет сохранен в безопасном месте. В дальнейшем его можно будет использовать для импорта.

ПРИМЕЧАНИЕ После создания или импорта пароль нельзя изменить.

Управление паролем шифрования

1. В области навигации слева выберите пункт **Политики**.

2. Выберите подпункт **Политика шифрования**.
3. Следуйте инструкциям на экране.

Определение количества поддерживаемых агентов

Сложно вывести общие правила, которые были бы справедливы для любой среды, поэтому приведенные здесь примеры содержат точное описание контекста, для которого применимы указанные значения.

Факторы, влияющие на масштабирование

Масштабирование среды Data Protector for PCs — это комплексная задача. Необходимо учесть следующие технические факторы, которые влияют на количество пользователей, поддерживаемых конкретной средой:

- вычислительная мощность Data Vault (для еженощной консолидации данных резервного копирования);
- пропускная способность сети и ввода-вывода на сервере Data Vault Server;
- дисковое пространство на сервере Data Vault Server;
- размер базы данных SQL на сервере Policy Server;
- пропускная способность сети на сервере Policy Server и его вычислительная мощность.

Какие из этих факторов могут стать «узким местом» конкретной среды зависит от следующих параметров конфигурации Data Protector for PCs и характера использования системы:

- число пользователей Data Vault;
- число и размер файлов, на которые распространяются настроенные политики защиты;
- частота изменения защищенных файлов;
- параметры хранения защищенных типов файлов.

Рекомендации по масштабированию

Data Vault

При ежедневном расписании очистки хранилище Data Vault с 14 ТБ дискового пространства сможет поддерживать до **3 500** агентов, если средние характеристики данных будут примерно следующими:

- среднее число защищенных файлов: 5000
- средний общий объем защищенных файлов на локальном диске: 10 ГБ;
- средний общий объем в Data Vault (после сжатия): 4 ГБ.

Если необходимо обеспечить защиту данных, объем которых в среднем больше, чем в этом примере, простое увеличение дискового пространства Data Vault позволит разместить больше данных, однако при этом может возникнуть ситуация, когда Data Vault уже не сможет своевременно выполнять консолидацию данных резервного копирования по ночам. Существует два варианта решения.

- Выполнение очистки Data Vault только по выходным. Инструкции см. в описании шага 2 «Настройка политики Cleanup» в разделе «Настройка остальных политик»(стр. 28). Таким образом при тех же средних характеристиках данных количество агентов, поддерживаемых Data Vault объемом 40 ТБ, можно будет увеличить до 10 000.
- Распределение данных пользователей между несколькими хранилищами Data Vault.

Ниже приведены характеристики оборудования для таких хранилищ Data Vault.

Тип Data Vault	Ежедневная очистка (до 3 500 агентов)	Еженедельная очистка (до 10 000 агентов)
Общая папка Windows	Двухъядерный процессор с частотой 3 ГГц, 4 ГБ ОЗУ, 14 ТБ дискового пространства	Двухъядерный процессор с частотой 3 ГГц, 4 ГБ ОЗУ, 40 ТБ дискового пространства
Web Data Vault	Четырехъядерный процессор с частотой 3 ГГц, 4 ГБ ОЗУ, 14 ТБ дискового пространства	Четырехъядерный процессор с частотой 3 ГГц, 4 ГБ ОЗУ, 40 ТБ дискового пространства

Если объем данных пользователей в среднем меньше, Data Vault сможет обслуживать больше пользователей, чем указано в этом примере.

ПРИМЕЧАНИЕ Для лучшей производительности компания HP настоятельно рекомендует размещать операционную систему хранилища Data Vault и данные резервного копирования на отдельных физических дисках.

Для лучшей производительности необходимо регулярно выполнять дефрагментацию диска Data Vault.

Policy Server

Объем трафика, создаваемого на сервере Policy Server, напрямую зависит от числа агентов, обслуживаемых этим сервером. При использовании выпуска MS SQL Server Express, который входит в комплект поставки Data Protector for PCs, максимальный размер базы данных составляет 4 ГБ, а максимальное число поддерживаемых агентов — 5 000[1] .

Если в среде необходимо обеспечить поддержку более 5 000 агентов, можно добавить дополнительные серверы Policy Server или заменить MS SQL Express на

1. При использовании указанного на сервере Policy Server срока хранения данных отчетности по умолчанию — 30 дней.

полнофункциональную версию Microsoft SQL Server. Таким образом Policy Server можно свободно масштабировать до 50 000 агентов. Если планируется использовать полнофункциональную версию MS SQL Server, объем основной памяти Policy Server следует увеличить как минимум до 3 ГБ.

По соображениям производительности серверы Policy Server и Data Vault Server должны работать на разных компьютерах. Их можно разместить на одном компьютере, но такой вариант рекомендуется только для пробного использования.

В среде должен быть хотя бы один сервер Policy Server, однако количество хранилищ Data Vault и серверов Policy Server не обязательно должно совпадать.

Рекомендации по использованию сети

ПРИМЕЧАНИЕ Высокая задержка в сети не влияет на работу хранилищ Web Data Vault. Данный раздел относится только к хранилищам Data Vault типа «общая папка Windows».

Как правило, компания HP не рекомендует выполнять начальное обновление хранилищ Data Vault типа «общая папка Windows» с агентов Data Protector for PCs, если задержка в сети между ними больше 50 мс. Эта рекомендация обычно относится к домашним и удаленным офисам с низкоскоростным подключением к глобальной сети. Начальное обновление будет выполняться, но очень медленно.

Если среда включает несколько офисов, расположенных в разных местах, и задержка в сети для некоторых из них больше 50 мс, установите хранилища Data Vault в нескольких местах, чтобы для всех офисов хотя бы одно хранилище Data Vault было достижимо с задержкой 50 мс или меньше.

После завершения начального обновления плановые обновления могут выполняться из любого места корпоративной сети или даже из домашнего офиса. Обычно они достаточно небольшие и не создают проблем даже при низкоскоростных сетевых подключениях.

Если для начального обновления нужно использовать подключение с высокой задержкой, на это может уйти несколько дней, однако его можно прервать без каких-либо потерь. При повторном подключении к Data Vault Data Protector for PCs продолжит обновление с того места, на котором оно было остановлено.

СОВЕТ Если задержка в сети между офисами неизвестна, используйте команду ping на компьютере в одном месте, чтобы проверить связь с компьютером в другом месте. Каждая успешная проверка связи возвращает значение задержки.

Глава 5. Настройка многопоточного режима Cleanup

Производительность программы DPNECleanup накладывает ограничение на объем пользовательских данных резервного копирования в Data Vault. Чтобы оптимизировать использование процессора и дискового пространства, эту программу можно настроить для работы в многопоточном режиме с возможностью повторного использования потоков и расширения. Это позволит хранить больший объем данных.

Если для многопоточного режима Cleanup указан аргумент планировщика «-s», используются аргументы по умолчанию «-e -f -u -p -d 1000», включая многопоточную очистку по умолчанию и задержку в 1 секунду для авторегулятора. Если не требуется использовать аргументы по умолчанию, например, чтобы отключить или настроить многопоточный режим, удалите из вызова планировщика аргумент «-s» и добавьте соответствующие аргументы командной строки.

ПРИМЕЧАНИЕ

Даже если при определённых обстоятельствах необходимо будет отключить многопоточный режим Cleanup, в вызове Cleanup для Data Vault рекомендуется оставить аргументы «-e -f -u».

Использование DPNECleanup.exe из командной строки

Аргумент -p программы DPNECleanup.exe позволяет инициализировать и запустить подсистему параллельной обработки и, таким образом, включить многопоточный режим. Подсистема параллельной обработки поддерживает семь необязательных аргументов командной строки. Исполняемый файл программы DPNECleanup принимает эти аргументы и передает их в подсистему параллельной обработки..

Если аргумент -p отсутствует, программа DPNECleanup запустится в последовательном режиме. В этом режиме не используется подсистема параллельной обработки.

dpnecleanup

–a *маскаСоответствия*

Задание маски соответствия процессоров равной указанному числу. Это число отражает установленные биты, соответствующие ядрам ЦП, которые должны использоваться потоками.

–d *задержка*

Задние задержки в миллисекундах перед началом работы авторегулятора, в результате чего подсистема параллельной обработки получает отсрочку запуска множества потоков и создания некоторой нагрузки на систему. По умолчанию аргумент –s вызывает задержку в 1000 миллисекунд или 1 секунду.

–m *максЗагрузкаЦП*

Задание требуемой максимальной загрузки ЦП (всех ядер, определяемых маской соответствия) в процентах, которой должен будет достичь авторегулятор. Значение

максЗагрузкаЦП должно быть целым числом в диапазоне от 1 до 100. По умолчанию используется значение «0», которое означает отсутствие ограничения, т. е. полную загрузку ЦП.

–o

Использование постоянного количества ресурсов. Это означает, что авторегулятор будет отключен и подсистема параллельной обработки не будет изменять количество параллельных потоков. Чтобы задать количество параллельных потоков, используйте аргумент –r. Аргументы –d, –m и –q не учитываются при использовании с аргументом –o.

–p

Включение многопоточного режима Cleanup.

–q *максДлинаОчереди*

Задание требуемой максимальной средней длины очереди диска, которой должен будет достичь авторегулятор. Значение должно быть числом с плавающей точкой По умолчанию используется значение «2.0».

–r *количествоРесурсов*

Задание количества одновременно используемых ресурсов (потоков) равным указанному числу. По умолчанию и в сочетании с параметром –o система использует 2^(количество ЦП) параллельных потоков. Если запущен авторегулятор, заданное значение будет означать максимальное количество одновременно используемых ресурсов, выраженное в потоках. По умолчанию максимальное количество равно «0», т. е. ограничение отсутствует.

–z [Idle | BelowNormal | Normal | AboveNormal | High | Realtime]

Задание приоритета процесса для всех потоков. По умолчанию используется значение Normal.

–s

Очистка на уровне сервера. Назначение очистки (Cleanup) для всех хранилищ Data Vault, как централизованных, так и локальных. При выполнении команды в многопоточном режиме заменяется аргументами «-e -f -u –p –d 1000».

–e

Очистка на уровне предприятия. Назначение очистки (Cleanup) для всех централизованных хранилищ Data Vault, которые указаны в политиках на сервере Policy Server.

–f

Быстрая очистка. Обычно программа Cleanup на агенте запускается, только когда система бездействует. Этот параметр позволяет программе Cleanup запускаться в любое время.

–u

Очистка на уровне пользователей. Назначение очистки (Cleanup) для всех локальных хранилищ Data Vault, которые указаны в локальных политиках, созданных пользователями.

Глава 6. Установка агентов Data Protector for PCs

ПРИМЕЧАНИЕ Лицензии распространяются на агенты при их установке.

Существует два способа установки агентов Data Protector for PCs.

- Установка на каждый клиентский компьютер по отдельности. См. раздел «Установка агентов Data Protector for PCs на клиентские компьютеры по отдельности»(стр. 38).
- Развертывание на предприятии с файлового сервера, доступного для всех клиентских компьютеров. См. раздел «Развертывание агентов Data Protector for PCs на предприятии»(стр. 39).

Установка агентов Data Protector for PCs на клиентские компьютеры по отдельности

Необходимые компоненты

Программное обеспечение агента Data Protector for PCs может быть установлено на настольных и переносных компьютерах пользователей, работающих под управлением ОС Windows. Поддерживаемые платформы см. в матрице поддержки.

Необходимо войти в систему с учетной записью, обладающей правами администратора.

Процедура установки

1. Вставьте установочный компакт-диск Data Protector for PCs. Мастер установки должен запуститься автоматически. В противном случае запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Выберите пункт **Установка/Обновление агента Data Protector for PCs**. Если появится диалоговое окно открытия или сохранения, выберите вариант **Открыть** (или **Запустить**).
3. Если на компьютере пользователя отсутствует установщик Microsoft Windows версии 3.1 или более поздней, мастер предложит его установить. Когда появится диалоговое окно обновления установщика Windows, нажмите кнопку **OK**, чтобы его установить.
4. Если на компьютере пользователя отсутствует платформа Microsoft .NET Framework 2.0 SP1 или более поздней версии, мастер предложит ее установить. Когда появится диалоговое окно установки платформы Microsoft .NET Framework 2.0 SP1, нажмите кнопку **OK**, чтобы ее установить.
5. Мастер автоматически установит агент Data Protector for PCs. Следуйте инструкциям на экране. Во время установки необходимо будет ввести сведения о Policy Server.

6. После завершения установки и настройки нажмите кнопку **Готово**. Если на сервере Policy Server задана политика Open File Protection, будет предложено перезагрузить компьютер.

   После этого в панели задач должен появиться значок Data Protector for PCs (один из следующих значков, в зависимости от статуса защиты: ).

7. Проверьте правильность работы агента Data Protector for PCs.
   a. Выберите или создайте тестовый файл, такой как документ Word или электронная таблица Excel, например, на рабочем столе. Внесите в него несколько изменений и нажмите кнопку **Сохранить**.
   b. Щелкните тестовый файл правой кнопкой мыши на рабочем столе, в проводнике или в диалоговом окне открытия. Открывшееся меню должно содержать три пункта Data Protector for PCs (**Поиск и восстановление файлов...**, **Копирование версии** и **Открыть версию с помощью *XXX*...**).
   c. Выберите пункт **Открыть версию с помощью *XXX*...**, после чего должен появиться список версий только что созданного или измененного документа с метками времени. Если выбрать одну из версий, она откроется как документ, доступный только для чтения, в соответствующем приложении. Таким образом пользователи восстанавливают предыдущие версии своих документов из локального репозитория Data Protector for PCs.

8. Повторите шаги 1–8 для остальных настольных и переносных компьютеров пользователей, которые необходимо защитить с помощью Data Protector for PCs.

Развертывание агентов Data Protector for PCs на предприятии

Для начального развертывания агентов Data Protector for PCs на предприятии можно воспользоваться пакетом развертывания агента Data Protector for PCs с установочного компакт-диска.

ПРИМЕЧАНИЕ Пакет развертывания нельзя использовать на компьютерах под управлением ОС Vista со включенным контролем учетных записей. Эта проблема решается путем отключения контроля учетных записей или установки агента в интерактивном режиме.

В описанной ниже процедуре сначала нужно скопировать пакет развертывания агента Data Protector for PCs из каталога *Компакт-диск*:\Agent в каталог на файловом сервере, который доступен всем пользователям. Затем с помощью программы SetupConfig.exe в этом каталоге создается файл параметров. В конце необходимо создать механизм для запуска программы StartInstall.exe в общем каталоге со всех компьютеров пользователей. Например, можно использовать сценарий входа. Процесс развертывания можно отслеживать с помощью отчета о развертывании агента в консоли Data Protector for PCs Policy Server Console.

Содержимое пакета

Пакет развертывания Data Protector for PCs содержит перечисленные ниже компоненты.

SetupConfig.exe	Используется для создания и изменения файла настройки.
StartInstall.exe	Используется для запуска программы Setup.exe с правами администратора.
Setup.exe	Используется для установки необходимых компонентов и файла DataProtectorNE.ini.
DataProtectorNE.msi	Пакет установщика Windows для Data Protector for PCs, используемый для установки программного обеспечения агента.
DataProtectorNE64.msi	Пакет установщика Windows для Data Protector for PCs, используемый для установки программного обеспечения агента на 64-разрядных компьютерах.
DataProtectorNE*.*.mst	Пакет установщика Windows для Data Protector for PCs, используемый для установки локализованного программного обеспечения агента.
WindowsInstaller.exe	Используется для обновления установщика Windows (требуется для установки .NET).
NetFx20SP1_x64.exe, NetFx20SP1_x86.exe	Используется для установки .NET Framework 2.0 SP1.
Setup.ini	Файл параметров настройки для установки Data Protector for PCs. Этот файл будет создан с помощью программы SetupConfig.exe (см. шаг 4 ниже).

Процедура развертывания и установки

1. Скопируйте файлы из каталога Agent на установочном компакт-диске в каталог, доступный всем пользователям, которые собираются использовать пакет развертывания агента Data Protector for PCs. Это может быть обычный общий ресурс сетевого доступа, например \\yourserver\DPNEDeploy.
2. Убедитесь, что созданный каталог содержит перечисленные выше файлы. Все остальные файлы можно удалить.
3. Откройте командное окно DOS (cmd.exe) и выполните команду cd, чтобы перейти в каталог, созданный на шаге 1.
4. Запустите программу SetupConfig.exe, чтобы создать или изменить файл параметров Setup.ini. При первом запуске программы SetupConfig.exe необходимо ввести значения для всех параметров. В дальнейшем программу SetupConfig.exe можно

будет запускать повторно для изменения параметров. Если параметры менять не нужно, просто нажмите клавишу **ВВОД**.

Ниже перечислены обязательные параметры.

- **UNC-путь к пакетам установки** — полный путь к общему каталогу, в который были скопированы файлы на шаге 1, например \\yourserver\DPNEDeploy.
- Имя **Data Protector for PCs Policy Server**. Можно указать NetBIOS-имя, например YOURSERVER, или полное доменное имя, например yourserver.yourcompany.com.
- **Имя пользователя** — имя пользователя с правами администратора на компьютерах, на которых используется пакет развертывания агента Data Protector for PCs, например члена группы администраторов домена. Обычно указывается полное имя пользователя, включающее домен, например YOURCOMPANY\JerryAdmin.
- **Пароль** — пароль, связанный с именем пользователя. Его необходимо ввести дважды для подтверждения.

5. На клиентском компьютере запустите программу StartInstall.exe, например \\yourserver\DPNEDeploy\StartInstall. Она в свою очередь запустит программу Setup.exe в фоновом режиме с низким приоритетом, используя имя пользователя и пароль, указанные в файле Setup.ini. Это действие может быть частью сценария входа. Учтите, что его нельзя включить в сценарий запуска, так как учетная запись компьютера не обладает достаточными сетевыми правами.
6. Программа Setup.exe проверит, поддерживает ли клиентский компьютер Data Protector for PCs. Поддерживаемые платформы Windows см. в матрице поддержки.
7. Программа Setup.exe проверит, установлена ли платформа .NET Framework 2.0 SP1. Если платформа не установлена, выполнится ее установка, после чего может потребоваться перезагрузить компьютер.
8. Программа Setup.exe проверит наличие уже установленного программного обеспечения Data Protector for PCs. Если ПО не установлено или его версия устарела, выполнится установка Data Protector for PCs.

ПРИМЕЧАНИЕ

Все ошибки, возникшие при выполнении шагов 4–7, записываются в журнал на сервере Data Protector for PCs Policy Server, а также в журнал событий приложений на локальном компьютере.

Ход развертывания агента можно проверить в консоли Data Protector for PCs Policy Server Console.

1. Войдите в консоль Data Protector for PCs Policy Server Console.

2. В области навигации слева разверните пункт **Отчеты** и выберите подпункт **Развертывание агента**.

   Откроется сводный отчет о начальном развертывании агента на текущий день. Он содержит следующие сведения:

   - число компьютеров, на которых успешно **завершено** развертывание;
   - число компьютеров, на которых **выполняется** развертывание;
   - число компьютеров, на которых произошел **сбой** развертывания.

3. Чтобы просмотреть список компьютеров с выбранным состоянием развертывания, щелкните число в столбце **Число компьютеров**.

   Отобразится текущий статус каждого компьютера. Например, если на каком-либо компьютере произошел сбой развертывания, столбец **Сведения** будет содержать сведения о возникшей ошибке. Чтобы получить дополнительные сведения о компьютере, нужно щелкнуть его NetBIOS-имя.

Глава 7. Обновление Data Protector for PCs

Обновление Data Protector for PCs 6.*x* до версии 7.0 выполняется в указанном ниже порядке.

1. Обновление Policy Server до версии 7.0. См. раздел «Обновление Policy Server»(стр. 43).
2. Установка Web Data Vault Server. См. «Установка, настройка и обслуживание Web Data Vault Server»(стр. 18).
3. Обновление агентов до версии 7.0.

   Их можно обновить вручную или автоматически с помощью политики обновления агента. Дополнительные сведения см. в разделе «Обновление агентов»(стр. 43).

Обновление Policy Server

Чтобы обновить версию уже установленного программного обеспечения Data Protector for PCs Policy Server, нужно следовать стандартной процедуре установки. В новой версии будут доступны все существующие конфигурации (такие как конфигурация Data Vault, лицензирование и т. д.).

Обновление Policy Server

1. Вставьте установочный компакт-диск Data Protector for PCs. Если мастер установки не запустился автоматически, запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Выберите пункт **Установка Policy Server** на странице мастера «Установка Data Protector for PCs», чтобы начать обновление.
3. Следуйте инструкциям на экране.
4. Мастер установки обнаружит установленное ПО Policy Server и предложит выполнить обновление.
5. Следуйте инструкциям на экране.
6. После завершения установки нажмите кнопку **Далее**. Затем можно запустить консоль Data Protector for PCs Policy Server Console.

ПРИМЕЧАНИЕ Если на сервере Policy Server установлено приложение Cleanup, его также необходимо обновить. Это можно сделать вручную или с помощью политики обновления агента.

Обновление агентов

Если обновить версию сервера Data Protector for PCs, существующие агенты, использующие предыдущую версию Data Protector for PCs, будут работать так же, как и прежде. Их можно обновить вручную или автоматически с помощью политики обновления агента.

ПРИМЕЧАНИЕ После обновления все агенты необходимо перезагрузить, чтобы они могли использовать новые хранилища Web Data Vault. Соответствующее предупреждение отобразится на ПК агентов в панели задач (в виде всплывающего сообщения), а также на вкладке «Сводка» панели «Работоспособность» в Data Protector for PCs.

Автоматическое обновление агентов с помощью политики обновления агента

Агенты можно обновить автоматически с помощью политики обновления агента, заданной на сервере Policy Server. Пакет установки будет автоматически доставлен на все подключенные клиенты, и обновление пройдет в автоматическом режиме. Участие пользователей при этом не требуется.

1. В консоли Policy Server Console выберите пункты **Политики -> Политика обновления агента**.
2. При обновлении Policy Server на сервер передается новый пакет обновления агента. В консоли Policy Server Console новая версия еще не выбрана.

   Выберите новую версию агента, чтобы она стала доступна.
3. В разделе регулирования можно изменить максимальное число обновлений, разрешенных в минуту.
4. Нажмите кнопку **Сохранить политику обновления агента**.
5. Агенты автоматически обновятся до самой последней версии. Агенты Cleanup также будут обновлены автоматически.

ПРИМЕЧАНИЕ Ход обновления агентов можно проверить с помощью следующего отчета: «Развертывание агента».

Ручное обновление агентов

Чтобы обновить версию существующего агента Data Protector for PCs, нужно выполнить стандартную процедуру установки.

Прежде чем обновлять агент до более новой версии, убедитесь, что версии агента и Data Protector for PCs Policy Server совместимы.

1. Вставьте установочный компакт-диск Data Protector for PCs. Если мастер установки не запустился автоматически, запустите его вручную, дважды щелкнув файл setup.hta в корне установочного компакт-диска.
2. Выберите пункт **Установка агента** на странице мастера «Установка Data Protector for PCs», чтобы начать обновление.
3. Следуйте инструкциям на экране.
4. Мастер установки обнаружит установленное ПО агента и предложит выполнить обновление
5. Следуйте инструкциям на экране.

Глава 8. Получение технической поддержки для Data Protector for PCs

Срок технической поддержки Data Protector for PCs составляет один год. Техническая поддержка предусматривает указанные ниже услуги.

- Техническая поддержка по телефону для консультации со специалистом.
- Предоставление обновлений программного обеспечения сервера Data Protector for PCs и агентов Data Protector for PCs. Последние версии или образ компакт-диска можно загрузить с веб-сайта Data Protector по адресу http://www.hp.com/go/dataprotector.

Глоссарий

Active Directory *(Термин Windows.)* Служба каталогов в сети Windows. Она содержит сведения о сетевых ресурсах и предоставляет пользователям и приложениям доступ к этим ресурсам. Службы каталогов обеспечивают единообразие именования, описания, размещения, доступа и управления для ресурсов независимо от их физического местонахождения.

Agent Программное обеспечение Data Protector for PCs, запущенное на всех настольных и переносных компьютерах пользователей. Оно обменивается данными с сервером Policy Server с помощью веб-служб (SOAP и XML) через TCP-порт 80.

Continuous File Protection Continuous File Protection — это метод постоянной защиты данных (Continuous Data Protection) в системе Data Protector for PCs, который обеспечивает автоматическое сохранение внесенных изменений при каждом сохранении файла. Он подходит для файлов данных, сохраняемых пользователем (в отличие от файлов, которые всегда открыты, таких как базы данных или файлы Outlook). Каждая политика Continuous File Protection защищает группу файлов, которые каким-то образом взаимосвязаны. Программное обеспечение Data Protector for PCs поставляется с настроенными политиками для распространенных типов файлов, таких как документы Office и рисунки. Можно изменить эти политики защиты файлов или создать собственные. Политика также определяет срок хранения предыдущих версий защищенных файлов.

Data Vault Хранилища Data Vault бывают двух типов.

- Хранилища Web Data Vault. Они используют протокол HTTPS и обеспечивают наивысший уровень безопасности при передаче данных между клиентскими компьютерами и Data Vault, а также лучшую пропускную способность в средах с высокой задержкой, и поэтому рекомендуются к использованию.
- Хранилища Data Vault типа «общая папка Windows». Это общие папки на файловом сервере, в которых файлы сохраняются в соответствии с политикой Data Vault. Файловый сервер должен поддерживать протокол совместного доступа к файлам Windows (CIFS/SMB). Такие хранилища не следует использовать в средах с высокой задержкой в сети.

Структура данных в хранилищах Data Vault обоих типов одинаковая, поэтому существующие хранилища Data Vault типа «общая папка Windows» можно преобразовать в хранилища Web Data Vault.

Пользователям можно назначить одно или несколько хранилищ Data Vault на основе их членства в группе или подразделении.

Local Repository Local Repository — это безопасное место для хранения защищенных файлов и их изменений на компьютерах агентов, которое обычно находится на системном жестком диске. Оно представляет собой скрытый системный каталог. Пользователи могут быстро восстановить предыдущую версию файла, щелкнув его правой кнопкой мыши на рабочем столе, в проводнике или в диалоговом окне открытия. Файлы, защищенные с помощью политик Continuous File Protection, хранятся в скрытом каталоге на локальном компьютере, пока не истечет срок хранения. Файлы, защищенные с помощью политик Open File Protection, временно хранятся в локальном хранилище версий, пока не будут скопированы в Data Vault. Обычно путь к Local Repository следующий: C:\{DPNE}.

Open File Protection Политика Open File Protection обеспечивает резервное копирование файлов, которые всегда открыты, таких как личные папки Outlook и многие файлы баз данных, периодически создавая снимки этих файлов. Этот метод иногда называют «почти» постоянной защитой данных (Continuous Data Protection). Политика Open File Protection устанавливает защиту для открытых файлов, определяемых наборами правил включения и исключения. Например, можно задать политику «Личные папки Outlook», применимую к PST-файлам Outlook, указав правило включения

«Заканчивается на .pst». Чтобы исключить архивные PST-файлы, можно создать правило исключения «Содержит archive». Политики также определяют срок хранения предыдущих версий защищенных файлов. Политики Open File Protection применяются ко всем пользователям.

Policy Server Сервер Policy Server обеспечивает централизованное управление политиками Data Protector for PCs. Он также осуществляет сбор данных о статусе агентов и предоставляет отчеты об их развертывании и работе.

Администратор Пользователь на сервере Web Data Vault Server, который выполняет административные задачи, такие как создание и удаление хранилищ Data Vault, а также миграция клиентских данных резервного копирования.

Защищенные файлы Защищенный файл — это файл, для которого автоматически выполняется резервное копирование с помощью Data Protector for PCs. Типы защищенных файлов определяются политиками Continuous File Protection и Open File Protection.

Консоль Отображаемая в браузере консоль используется для централизованного определения политик Data Protector for PCs. Для этого нужно быть членом группы «Администраторы».

Начальное обновление Программное обеспечение Data Protector for PCs обеспечивает постоянную защиту файлов, сохраняя изменения по мере их внесения. При создании нового хранилища Data Vault в нем необходимо выполнить начальное обновление всех защищенных файлов пользователей с помощью Data Protector for PCs. Пользователи могут выбрать способ выполнения начального обновления: немедленно или в фоновом режиме.

Политика Политика — это набор правил, централизованно определенных на сервере Policy Server и выполняемых агентами на всех настольных и переносных компьютерах.

Политика Cleanup Сроки хранения, определяемые политиками защиты файлов, соблюдаются за счет периодически выполняемых задач очистки. Их частота задается в политике Cleanup. По умолчанию очистка пользовательских репозиториев Local Repository выполняется каждый час, а локальных хранилищ Data Vault — раз в день. Для очистки хранилищ Data Vault типа «общая папка Windows» используется компьютер, назначенный в политике Data Vault, а для очистки хранилищ Web Data Vault — приложение Cleanup, запущенное локально на сервере Data Vault Server. Политика Cleanup применяется ко всем пользователям.

Политика копирования Политики копирования определяют указанные ниже параметры.

- Число агентов, которые могут одновременно копировать файлы в хранилища Data Vault.
- Расписание периодических обновлений, которое обеспечивает проверку наличия всех предполагаемых файлов пользователей в Data Vault и копирование отсутствующих файлов. Это дополнительно гарантирует правильность копирования всех файлов пользователей в Data Vault.
- Необходимость выполнения *начального обновления*. Начальное обновление является необходимым, так как при нормальной работе Data Protector for PCs каждый раз, когда пользователь изменяет файл, который находится под постоянной защитой Data Protector for PCs, в Data Vault копируются только сведения об изменениях.

Сразу после установки Data Protector for PCs нужно задать политику копирования, чтобы выполнить начальное обновление всех защищенных файлов пользователей.

Политика управления пользователями

Эта политика определяет полномочия отдельных пользователей в отношении программного обеспечения агента, запущенного на их настольных и переносных компьютерах. Можно заблокировать агент так, чтобы политики были полностью скрыты от пользователей, или разрешить им просматривать политики, но не изменять их, или позволить добавлять собственные политики.

Уровень полномочий можно задать для каждой из основных политик Data Protector for PCs в отдельности. Политика управления пользователями применяется ко всем пользователям.

Пользователь, выполняющий резервное копирование

Пользователь на сервере Web Data Vault Server, который выполняет пользовательские операции, такие как резервное копирование и восстановление файлов.

Указатель

Л

М

Н

О

П

Р

С