

HP Data Protector for PCs 7.0

Installations- und Administrationshandbuch

HP Teilenummer: n. z.
Ausgabedatum: Juni 2011
Ausgabe: Erste



© Copyright 2011 Hewlett-Packard Development Company, L.P.

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212; kommerzielle Computersoftware, Computersoftwareokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Die in diesem Dokument enthaltenen Informationen können jederzeit ohne Ankündigung geändert werden. Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. HP übernimmt keine Haftung für technische oder redaktionelle Fehler oder für die Vollständigkeit der Angaben in diesem Dokument.

Microsoft®, Windows®, Windows NT®, Windows® XP und Windows Vista® sind in den Vereinigten Staaten eingetragene Marken der Microsoft Corporation.

Inhalt

Informationen zu diesem Dokument.....	5
Zielgruppe.....	5
Dokumentkonventionen und -symbole.....	5
Allgemeine Informationen.....	6
HP, Technischer Support.....	6
Abonnementservice.....	6
HP Websites.....	7
Dokumentations-Feedback.....	7
1 Übersicht und Voraussetzungen.....	8
Übersicht zu Data Protector for PCs.....	8
Data Vaults.....	9
Handhabung von Zertifikaten.....	10
Selbstsignierte Zertifikate.....	10
Importierte Zertifikate.....	10
Austauschen des Zertifikats.....	11
Data Protector for PCs installieren – Übersicht.....	11
Voraussetzungen.....	12
Richtlinienserver.....	12
Datenbank.....	13
Data Protector for PCs – Web-Data Vault-Server.....	13
Data Protector for PCs-Agenten.....	13
2 Policy Server von Data Protector for PCs installieren.....	14
Schnellinstallation.....	14
Benutzerdefinierte Installation.....	15
3 Installieren, Konfigurieren und Verwalten des Web-Data Vault-Servers.....	18
Installieren und Konfigurieren des Web-Data Vault-Servers.....	18
Verwalten der Web-Data Vaults.....	19
Migrieren von Daten eines Data Vaults in einer Windows-Dateifreigabe in einen Web-Data Vault.....	20
Optionen für Web-Data Vaults über die Befehlszeilenschnittstelle (DvConfig) konfigurieren.....	21
4 Data Protector for PCs-Schutzrichtlinien konfigurieren.....	23
Ersteinrichtung nach der Installation von Data Protector for PCs.....	23
Erstkonfiguration.....	24
Weitere Richtlinien konfigurieren.....	28
Weitere Konfigurationsschritte.....	30
Anzahl der Agents bestimmen, die unterstützt werden können.....	32
Einflussfaktoren beim Sizing.....	32
Sizing-Empfehlungen.....	32
Data Vault.....	32

Richtlinienserver.....	33
Netzwerkfaktoren.....	34
5 Konfigurieren des Multithread-Cleanup.....	35
DPNECleanup.exe über die Befehlszeilenschnittstelle verwenden.....	35
6 Data Protector for PCs-Agenten installieren.....	37
Data Protector for PCs-Agenten auf einzelnen Clientcomputern installieren.....	37
Voraussetzungen.....	37
Installationsprozedur.....	37
Data Protector for PCs-Agents unternehmensweit bereitstellen.....	38
Inhalt des Kits.....	39
Bereitstellungs- und Installationsprozedur.....	39
7 Aktualisieren von Data Protector for PCs.....	42
Policy Server aktualisieren.....	42
Agenten aktualisieren.....	42
Agenten automatisch über die Agentenaktualisierungsrichtlinie aktualisieren.....	43
Manuelle Aktualisierung von Agenten.....	43
8 Support für Data Protector for PCs anfordern.....	45
Glossar.....	46
Stichwortverzeichnis.....	49

Informationen zu diesem Dokument

In diesem Handbuch sind Informationen zu Folgendem enthalten:

- Installation von HP Data Protector for PCs
- Konfiguration von Richtlinien für HP Data Protector for PCs
- HP Data Protector for PCs-Agentensoftware auf Desktop-PCs und Notebooks von Benutzern
- Bestimmung der Anzahl an Agents, die unterstützt werden können
- Anfordern von Support für Data Protector for PCs

Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die HP Data Protector for PCs installieren und konfigurieren möchten. Es werden folgende Kenntnisse empfohlen:

- Windows-Administration

Dokumentkonventionen und -symbole

Konvention	Element
Blauer Text: „ Informationen zu diesem Dokument “ (Seite 5)	Querverweise und E-Mail-Adressen
Blauer unterstrichener Text: http://www.hp.com	Websiteadressen
Fettgedruckter Text	<ul style="list-style-type: none">• Zu drückende Tasten• Text, der in der grafischen Benutzeroberfläche eingegeben wird, z. B. in einem Feld• Elemente der grafischen Benutzeroberfläche, die angeklickt oder ausgewählt werden, z. B. Menüs, Listeneinträge, Schaltflächen, Registerkarten und Kontrollkästchen
<i>Kursivgedruckter</i> Text	Hervorgehobener Text

Konvention	Element
Monospace-Text	<ul style="list-style-type: none"> • Datei- und Verzeichnisnamen • Systemausgaben • Code • Befehle, ihre Argumente und Argumentwerte
<i>Kursivgedruckter Monospace-Text</i>	<ul style="list-style-type: none"> • Codevariablen • Befehlsvariablen
Fettgedruckter Monospace-Text	Hervorgehobener Monospace-Text

ⓘ **WICHTIG:** Kennzeichnet erklärende Informationen oder spezielle Anweisungen.

HINWEIS: Kennzeichnet zusätzliche Informationen.

Allgemeine Informationen

Allgemeine Informationen zu Data Protector for PCs finden Sie unter <http://www.hp.com/go/dataprotector>.

HP, Technischer Support

Informationen zum weltweiten technischen Support finden Sie auf der HP Support-Website: <http://www.hp.com/support>

Stellen Sie die folgenden Informationen zusammen, bevor Sie sich an HP wenden:

- Modellnamen und -nummern der Produkte
- Registrierungsnummer beim technischen Support (falls zutreffend)
- Seriennummern der Produkte
- Fehlernachrichten
- Typ und Versionsstufe des Betriebssystems
- Detaillierte Fragen

Abonnementservice

HP empfiehlt, dass Sie Ihr Produkt auf der Website „Subscriber’s Choice for Business“ registrieren:

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

Nach der Registrierung erhalten Sie E-Mail-Benachrichtigungen über Produktverbesserungen, neue Treiberversionen, Firmwareaktualisierungen und andere Produktressourcen.

HP Websites

Weitere Informationen finden Sie auf den folgenden HP Websites:

- <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>

Dokumentations-Feedback

HP freut sich über Ihr Feedback.

Wenn Sie Anmerkungen oder Vorschläge zu Produktdokumentation einreichen möchten, senden Sie eine Nachricht an DP.DocFeedback@hp.com. Alle Einreichungen werden Eigentum von HP.

1 Übersicht und Voraussetzungen

Übersicht zu Data Protector for PCs

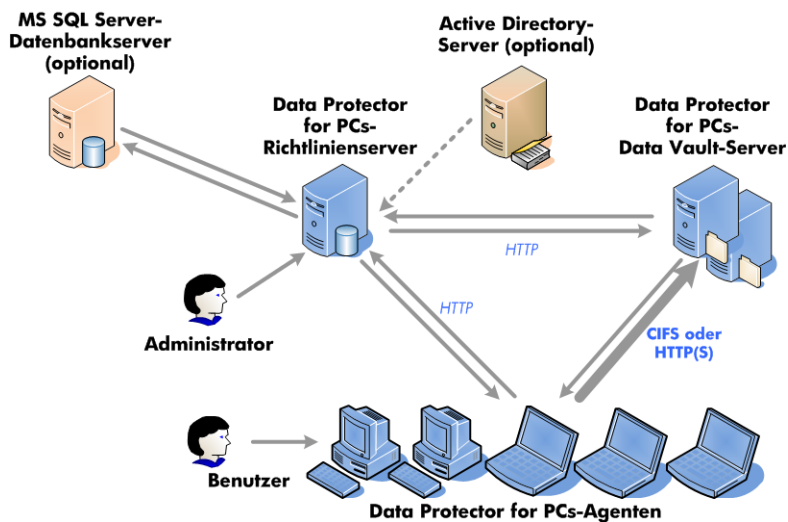
HP Data Protector for PCs besteht im Wesentlichen aus zwei Softwarekomponenten, dem Policy Server und den Agenten. Der Policy Server wird auf einem Windows-Server ausgeführt. Informationen zu unterstützten Versionen finden Sie in der Unterstützungsmatrix (<https://h20230.www2.hp.com/selfsolve/manuals>). Die Agenten werden auf den einzelnen Desktop-PCs und Notebooks im Hintergrund ausgeführt.

Der Policy Server kann auch auf Gruppen und Organisationseinheiten auf einem Active Directory Server zugreifen.

Benutzerdaten werden in Data Vaults gesichert. Der Data Vault-Server sollte sich getrennt vom Policy Server befinden. Wenn Sie Data Vaults in Windows-Dateifreigaben anstelle der empfohlenen Web-Data Vaults verwenden, befinden sich diese in einer oder mehreren Windows-Dateifreigaben auf Dateiservern.

In der folgenden Abbildung ist die Data Protector for PCs-Architektur dargestellt:

Abbildung 1 Architektur von Data Protector for PCs



In den verschiedenen Richtlinien ist festgelegt, welche Dateien von den Desktop-PCs und Notebooks gesichert werden und wo diese Sicherungen gespeichert werden. Die Richtlinien werden in der Policy Server Console definiert. Anschließend werden die Richtlinien automatisch mithilfe des SOAP-Protokolls über HTTP-Port 80 an die Agenten verteilt. Die Richtlinien werden auf dem Policy Server aufbewahrt.

Die Agenten führen diese Richtlinien aus. Wenn ein Benutzer eine Datendatei ändert, die gemäß einer der Richtlinien geschützt wird, wird auf der lokalen Festplatte des

Desktop-PCs oder Notebooks eine Vorgängerversion erstellt, und Änderungen an der Datei werden komprimiert und auf die entsprechenden Data Vaults kopiert.

Wenn Dateien gesichert werden, benachrichtigt der Agent den Policy Server, der ein Prüfprotokoll der von Benutzern vorgenommenen Änderungen enthält. Zusätzlich sendet jeder Agent regelmäßig Statusinformationen an den Policy Server. Berichte zu diesen Daten können über die Policy Server Console generiert werden.

Data Vaults befinden sich auf dem Data Vault-Server. Clientdaten werden mithilfe der beiden folgenden Protokolle in die Data Vaults kopiert: CIFS (für Data Vaults in Windows-Dateifreigaben) oder HTTP (für Web-Data Vaults).

Der Data Vault-Server sollte sich auf einem anderen System befinden als der Policy Server. Im Fall von HTTPS wird die Web-Data Vault-Serversoftware zusammen mit der Cleanup-Software von Data Protector for PCs darauf ausgeführt. Im Fall von Data Vaults in Windows-Dateifreigaben ist nur die Cleanup-Software darauf installiert.

Wenn Sie Active Directory verwenden, können Sie den Policy Server so konfigurieren, dass er auf Ihre Gruppen und Organisationseinheiten zugreift. Anschließend können Sie den Benutzern auf der Grundlage ihrer Zugehörigkeit zu Gruppen oder Organisationseinheiten Data Vaults zuweisen. Auch in Berichten können Sie Benutzer auf der Grundlage ihrer Zugehörigkeit auswählen.

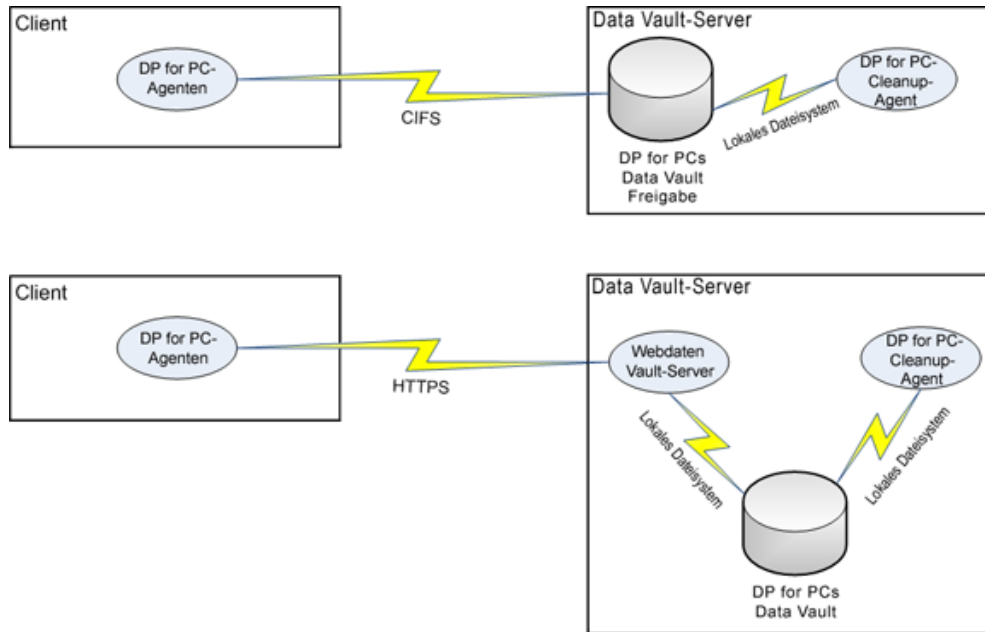
Data Vaults

Es gibt zwei verschiedene Arten von Data Vaults, die mit Data Protector for PCs verwendet werden können:

- Web-Data Vaults – basierend auf dem HTTPS-Protokoll. Diese bieten höchste Sicherheit und höheren Durchsatz in Umgebungen mit hoher Latenz und werden daher empfohlen.
- Data Vaults in Windows-Dateifreigaben – basierend auf dem CIFS-Protokoll, wurden in früheren Versionen von Data Protector for PCs verwendet.

Die Datenstruktur beider Data Vault-Typen ist identisch, sodass Sie bestehende Data Vaults in Windows-Dateifreigaben in Web-Data Vaults konvertieren können.

Abbildung 2 Vergleich zwischen Data Vaults in Windows-Dateifreigaben und Web-Data Vaults



Handhabung von Zertifikaten

Bei Web-Data Vaults muss SSL verwendet werden. Die Art des Zertifikats wird während der Installation des Web-Data Vault festgelegt. Wenn Sie ein Produkt bereitstellen möchten, das sofort einsatzbereit ist, beispielsweise zu Bewertungszwecken, können Sie den Web-Data Vault-Server mit einem selbstsignierten Zertifikat installieren. Ein solches Zertifikat ist nicht so sicher wie ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben wird. Wenn Sie umfassende Sicherheit benötigen, importieren Sie für den Data Vault-Server ein Zertifikat, das von einer für Ihre Umgebung vertrauenswürdigen Zertifizierungsstelle signiert ist, und fügen dieses zur Serverkomponente hinzu.

Selbstsignierte Zertifikate

Wenn Sie eine Data Vault-Richtlinie erstellen, können Sie festlegen, ob ein selbstsigniertes Zertifikat zulässig ist. Seitens des Agenten ist in diesem Fall keine Aktion erforderlich. Ein durch die Installation ausgestelltes selbstsigniertes Zertifikat hat eine Laufzeitbeschränkung von 20 Jahren.

Importierte Zertifikate

Beim Importvorgang wird eine einzelne Datei im PEM-Format erwartet, die sowohl den privaten Schlüssel als auch das passende Zertifikat mit dem öffentlichen Schlüssel enthält. Beachten Sie, dass die Datei unverändert in das Konfigurationsverzeichnis des Web-Data

Vault-Servers kopiert wird. Je nachdem, mit welchem Verfahren die Zertifikatsdatei erstellt wurde, ist diese Datei möglicherweise verschlüsselt. In diesem Fall wird von dem Windows-Dienstprozess, der den Web-Data Vault-Server ausführt, eine interaktive Eingabeaufforderung zur Eingabe des Passworts zum Entschlüsseln angezeigt. Dieser Fall tritt während der Installation und zudem bei jedem zukünftigen Neustart des Dienstes ein, beispielsweise nach einem Systemneustart. Sie können das Passwort zwar manuell zur Konfigurationsdatei des Webserver hinzufügen, um die Eingabeaufforderung zu vermeiden, dieser Vorgang wird jedoch bei der Installation nicht unterstützt. Es ist nicht ratsam, das Passwort für eine verschlüsselte Zertifikatsdatei in einer benachbarten Datei zu speichern.

HINWEIS:

Der Begriff „Vertrauenswürdige Zertifizierungsstelle“ bedeutet, dass die Clientcomputer, auf denen die Agenten ausgeführt werden, diese Zertifizierungsstelle für vertrauenswürdig halten und dass sie deren signierte Zertifikate akzeptieren. Hierbei wird davon ausgegangen, dass der Windows-Zertifikatspeicher auf den Clientcomputern bereits entsprechend eingerichtet wurde, indem das Zertifikat der Zertifizierungsstelle sowie möglicherweise weitere Zertifikate in der Kette hinzugefügt wurden. Der Agent selbst weist keinen Mechanismus auf, um diesen Vorgang durchzuführen. Er verlässt sich auf den Windows-Mechanismus.

Austauschen des Zertifikats

Sie können das Zertifikat auf dem Web-Data Vault-Server jederzeit nach der Installation mit dem Dienstprogramm `DvConfig` austauschen. Dieser Vorgang wird im Abschnitt zur Befehlszeilenschnittstelle unter „[Optionen für Web-Data Vaults über die Befehlszeilenschnittstelle \(DvConfig\) konfigurieren](#)“ (Seite 21) näher beschrieben. Sie können beispielsweise eine Installation, die ursprünglich mit einem selbstsignierten Zertifikat eingerichtet wurde, so umkonfigurieren, dass ein importiertes Zertifikat verwendet wird.

Data Protector for PCs installieren – Übersicht

HINWEIS: Weitere Informationen zur Aktualisierung einer Installation von Data Protector for PCs finden Sie in „[Aktualisieren von Data Protector for PCs](#)“ (Seite 42).

Die Installation von Data Protector for PCs umfasst drei Schritte:

1. **Installieren Sie den Policy Server von Data Protector for PCs.**
Siehe „[Policy Server von Data Protector for PCs installieren](#)“ (Seite 14).
2. **Installieren Sie die Web-Data Vault-Serversoftware für Data Protector for PCs.**
Siehe „[Installieren, Konfigurieren und Verwalten des Web-Data Vault-Servers](#)“ (Seite 18).

3. Konfigurieren Sie Schutzrichtlinien.

Siehe „Data Protector for PCs-Schutzrichtlinien konfigurieren“ (Seite 23).

4. Installieren Sie Data Protector for PCs-Agenten auf Laptops und Desktop-PCs.

Siehe „Data Protector for PCs-Agenten installieren“ (Seite 37).

Voraussetzungen

Richtlinienserver

Informationen zu unterstützten Betriebssystemen finden Sie in der Unterstützungsmatrix.

HINWEIS: *Installation unter Windows 2003 mit 64 Bit:* Der Policy Server wird unter 64-Bit-Windows-Betriebssystemen im 32-Bit-Kompatibilitätsmodus ausgeführt. Das bedeutet, dass ISS (Internet Information Services) im 32-Bit-Modus ausgeführt werden muss. Ist dies nicht der Fall, wird dies beim Überprüfen der Voraussetzungen während der Installation erkannt. Dann erhalten Sie die Möglichkeit, IIS in den 32-Bit-Modus zu versetzen. Wenn andere Webanwendungen auf dem Server die Ausführung von IIS im 64-Bit-Modus erfordern (z. B. Microsoft Exchange 2007 mit Webmail – Outlook Web Access), können Sie den Policy Server nicht auf diesem Server installieren. Dies gilt nicht für die Installation eines Policy Server unter Windows 2008.

Auf dem Server muss Folgendes installiert sein:

- Internet Information Services 6.0, 7.0, 7.5 oder neuere Version mit Unterstützung für ASP.NET-Anwendungen.

Für Windows 2003 ist IIS 6.0 eine Voraussetzung und muss installiert sein, bevor der Policy Server installiert werden kann. Für Windows 2008 bietet Data Protector for PCs die Installation von IIS 7.0 und 7.5 an, falls diese Versionen noch nicht installiert sind.

- Microsoft ASP.NET 2.0

Außerdem muss Folgendes auf dem Server installiert sein.

- Microsoft Installer 3.1 oder neuere Version (erforderlich für .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 oder neuere Version. Der Assistent installiert Version 2.0 SP1.
- Microsoft SQL Express (wenn keine andere SQL-Version vorhanden ist)

Außerdem werden (nur für Internet Information Services 7.0 und 7.5) die folgenden IIS-Komponenten benötigt. Wenn diese nicht installiert sind, können Sie sie mithilfe des Assistenten installieren:

- IIS Static Content Web Server – erforderlich für das Abrufen statischer HTML-Dateien, Dokumente und Bilder.

- IIS ASP.NET – erforderlich für die Bereitstellung von ASP.NET 2.0 und .NET Framework.
- IIS Security – erforderlich zur Nutzung der integrierten Windows-Authentifizierung für die Policy Server Console.
- IIS 6 Management Compatibility – ermöglicht, dass IIS 6 und IIS 7 beim Einrichten so identisch wie möglich konfiguriert werden.

Datenbank

Data Protector for PCs benötigt Zugriff auf eine Microsoft SQL Server-Datenbank. Informationen zu unterstützten Versionen finden Sie in der Unterstützungsmatrix.

Mithilfe von Microsoft Enterprise Manager können Sie den Authentifizierungsmodus Ihrer SQL Server-Installation wie folgt ermitteln (und ändern):

1. Klicken Sie mit der rechten Maustaste auf die SQL Server-Instanz, wählen Sie **Eigenschaften** aus, und klicken Sie auf die Registerkarte **Sicherheit**.
2. Die Option **SQL Server- und Windows-Authentifizierungsmodus** sollte bereits ausgewählt sein (nicht ausschließlich die Windows-Authentifizierung). Ist dies nicht der Fall, wählen Sie die Option aus, und klicken Sie auf **OK**.

Alternativ können Sie während der Installation von Data Protector for PCs eine Instanz von Microsoft SQL Server Express Edition installieren.

Data Protector for PCs – Web-Data Vault-Server

- Der Web-Data Vault-Server sollte in einem anderen System installiert werden als der Policy Server. (Beide Server können im selben System installiert werden. Diese Vorgehensweise ist jedoch nur zu Bewertungszwecken geeignet.)
- Java Runtime-Umgebung Version 1.6 oder eine neuere Version muss installiert sein.
- Die Variablen `JAVA_HOME` und `JRE_HOME` müssen auf das Java Runtime-Installationsverzeichnis verweisen.

Data Protector for PCs-Agenten

Data Protector for PCs-Agentensoftware kann auf Desktop-PCs und Notebooks von Benutzern mit Windows installiert werden. Informationen zu unterstützten Plattformen finden Sie in der Unterstützungsmatrix.

2 Policy Server von Data Protector for PCs installieren

HINWEIS: Sie können die vorhandene Installation eines Data Protector for PCs-Policy Server mithilfe der Standard-Installationsprozedur auf eine neuere Version aktualisieren. Weitere Informationen finden Sie unter „[Policy Server aktualisieren](#)“ (Seite 42).

Schnellinstallation

Die Anforderungen für den Data Protector for PCs-Policy Server finden Sie unter „[Richtlinienserver](#)“ (Seite 12).

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Befolgen Sie die angezeigten Anweisungen.
3. Der Data Protector for PCs-Policy Server benötigt Zugriff auf eine Microsoft SQL Server-Datenbank. Wählen Sie **Vorhandene Data Protector for PCs-Instanz von Microsoft SQL Server Express verwenden** oder **Vorhandene Instanz von Microsoft SQL Server verwenden** aus. Wenn Sie auswählen, dass ein vorhandener SQL-Server verwendet werden soll, müssen Sie die Verbindungszeichenfolge für den Datenbankserver und Anmeldeinformationen für ein Konto mit ausreichenden Rechten zum Erstellen einer neuen Datenbank angeben.
4. Klicken Sie auf der Assistentenseite für die Installation des Data Protector for PCs-Policy Server auf **Installieren**, um die Installation zu starten.
5. Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**. Anschließend können Sie die Policy Server Console von Data Protector for PCs starten.
6. Installieren Sie den Web-Data Vault-Server in einem separaten System. Klicken Sie auf dem Hauptinstallationsbildschirm auf **Data Vault installieren**.

HINWEIS: Bei der Installation wird die Cleanup-Software immer zusammen mit der Web-Data Vault-Serversoftware installiert. Bei einem Data Vault-Server, der als Host nur Data Vaults in Windows-Dateifreigaben enthält, empfiehlt es sich, die Installation lokal im Data Vault vorzunehmen, um die Leistung zu optimieren.

Benutzerdefinierte Installation

HINWEIS:

Nur Windows 2003-Server: Sie können den Data Protector for PCs-Policy Server nur von einer gemeinsam im Netzwerk genutzten CD-ROM oder von einer Netzwerkdateifreigabe installieren, wenn die Laufzeitsicherheitsrichtlinie für NET 2.0 Framework bei diesem Server auf *Voll vertrauenswürdig* für die Sicherheitszone „Lokales Intranet“ festgelegt ist. Wenn Ihr Server nicht über ein lokales CD-ROM-Laufwerk verfügt, ändern Sie die Laufzeitsicherheitsrichtlinie für die Sicherheitszone „Lokales Intranet“ mithilfe des in den Verwaltungstools enthaltenen Konfigurationstools für .NET Framework 2.0 in *Voll vertrauenswürdig*, oder kopieren Sie den Ordner „Server“ von der CD auf eine lokale Festplatte auf dem Server.

Um die Installation des Data Protector for PCs-Policy Server durchführen zu können, müssen Sie bei einem Konto mit Administratorrechten angemeldet sein.

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf **Policy Server installieren**.
Wenn eine entsprechende Abfrage angezeigt wird, wählen Sie **Öffnen** (oder **Ausführen**) aus, um das Programm an der aktuellen Speicherposition zu öffnen bzw. auszuführen. Wählen Sie nicht die Option zum Speichern des Programms auf der Festplatte aus.
3. Der Data Protector for PCs-Policy Server erfordert .NET Framework 2.0 SP1. Wenn dies noch nicht installiert ist, werden Sie gefragt, ob Sie es von der CD-ROM installieren möchten.
Die Installation erfordert Windows Installer 3.1 oder eine neuere Version. Falls dies nicht installiert ist, werden Sie gefragt, ob Sie Windows Installer 3.1 von der CD installieren möchten.
4. Der Installationsassistent prüft, ob die weitere erforderliche Software installiert ist:
 - Internet Information Services (IIS)
 - ASP.NET 2.0

Wenn eine dieser Komponenten fehlt, klicken Sie auf den entsprechenden Eintrag in der Liste, um Informationen zur Installation zu erhalten.

Klicken Sie auf **Weiter**.

5. Installieren Sie Microsoft SQL Server.

Gehen Sie wie folgt vor, um eine vorhandene Instanz von Microsoft SQL Server zu verwenden:

- a.** Klicken Sie auf **Vorhandene Instanz von Microsoft SQL Server verwenden**.
- b.** Geben Sie im Feld **Datenbankserver** die Verbindungszeichenfolge für den vorhandenen Datenbankserver ein.
- c.** Geben Sie in den Feldern **Benutzername** und **Passwort** die Anmeldedaten für ein Konto mit ausreichenden Rechten zum Erstellen einer neuen Datenbank ein. In der Regel ist dies das Konto für den Systemadministrator.
- d.** Klicken Sie auf **Weiter**. Mit den eingegebenen Verbindungsinformationen wird die Verbindung zum vorhandenen Datenbankserver getestet. Wenn der Verbindungstest erfolgreich ist, geht der Assistent zu Schritt 6 über.

So installieren Sie die Data Protector for PCs-Instanz von Microsoft SQL Server Express Edition:

- a.** Wählen Sie **DataProtectorNE-Instanz von Microsoft SQL Server Express installieren** aus, und klicken Sie auf **Weiter**.
- b.** Klicken Sie auf **Installieren**, um eine Instanz von Microsoft SQL Server 2005 Express Edition mit der Bezeichnung „DataProtectorNE“ zu installieren. Klicken Sie auf **Weiter**, wenn die Installation abgeschlossen ist.

6. Installieren Sie die Software für den Data Protector for PCs-Policy Server.

- a.** Klicken Sie auf der Eingangsanzeige auf **Weiter**, um die Installation zu starten.
 - Die Policy Server Console von Data Protector for PCs wird als Webanwendung im virtuellen Verzeichnis `C:\Inetpub\wwwroot\dpnepolicy` installiert.
 - Der Data Protector for PCs-Webservice wird unter `C:\Inetpub\wwwroot\dpnepolicyservice` installiert.

Beide verwenden das HTTP-Protokoll an Port 80.

- b.** Klicken Sie auf **Schließen** und **Weiter**, wenn die Installation des Policy Server abgeschlossen ist.

7. Anschließend muss das Cleanup-Programm installiert werden. Klicken Sie auf **Installieren**, um die Installation zu starten.

8. Wenn die Cleanup-Installation abgeschlossen ist, klicken Sie auf **Weiter**.

Data Protector for PCs wird zentral über die Policy Server Console von Data Protector for PCs verwaltet. Da die Konsole browserbasiert ist, können Sie Data Protector for PCs von jedem Computer aus verwalten, der eine Browserverbindung zum Policy Server herstellen kann (über HTTP-Port 80).

Um die Policy Server Console von Data Protector for PCs mit einem Browser auf dem Policy Server auszuführen, lassen Sie das Kontrollkästchen **Policy Server Console ausführen** aktiviert, und klicken Sie auf **Fertig stellen**.

HINWEIS: Während der Installation wird auf dem Policy Server die Cleanup-Software installiert. Zur Optimierung der Leistung wird empfohlen, diese auch in den Data Vaults zu installieren.

HINWEIS:

Browsereinstellungen für die Policy Server Console: Wenn Sie Probleme haben, die Seiten der Policy Server Console in Ihrem Browser anzuzeigen, überprüfen Sie die Sicherheitseinstellungen des Browsers. Die Konsole erfordert Folgendes:

- JavaScript muss aktiviert sein.
- Der Popup-Blocker muss für die dpnepolicy-Website deaktiviert sein.
- Möglicherweise müssen Sie weitere einschränkende Sicherheitseinstellungen ändern, abhängig von Ihrem Browser und dessen Version.

Installation mit Microsoft SharePoint: Beim Installieren des Policy Server auf einem Server, auf dem Microsoft SharePoint ausgeführt wird, tritt beim Starten der Policy Server Console möglicherweise der Fehler 404 auf (Seite kann nicht gefunden werden). Dieses Problem und seine Lösung werden in einem Artikel der Microsoft-Wissensdatenbank unter <http://support.microsoft.com/kb/828810> beschrieben. Beachten Sie, dass dieses Problem alle ASP.NET-Webanwendungen betrifft, nicht nur den Policy Server.

Gehen Sie wie folgt vor, damit der Policy Server auf einem Server mit SharePoint ausgeführt werden kann:

1. Verwenden Sie die SharePoint-Administrationstools, um Ausschlüsse für die zwei Webanwendungen des Policy Server zu erstellen: dpnepolicy und dpnepolicyservice.
 2. Ändern Sie die beiden web.config-Dateien des Policy Server (dpnepolicy\web.config und dpnepolicyservice\web.config), um den XML-Code <httpHandlers> und <trust> hinzuzufügen, wie im zuvor angegebenen Artikel der Microsoft-Wissensdatenbank beschrieben.
-

3 Installieren, Konfigurieren und Verwalten des Web-Data Vault-Servers

Installieren und Konfigurieren des Web-Data Vault-Servers

HINWEIS: Installieren Sie den Web-Data Vault-Server in einem anderen System als den Policy Server. (Beide Server können im selben System installiert werden. Diese Vorgehensweise ist jedoch nur zu Bewertungszwecken geeignet.)

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf **Data Vault installieren**.
3. Wählen Sie zwischen den folgenden Optionen:
 - **Web-Data Vault-Server** (empfohlen). Hierbei wird auch die Cleanup-Software auf dem Server installiert.
 - **Cleanup-Software für Windows-Dateifreigabe**. Wählen Sie diese Option aus, wenn Sie nur Data Vaults in Windows-Dateifreigaben verwenden möchten.

Weitere Informationen finden Sie unter „Data Vaults“ (Seite 9).

4. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen.
5. Wenn Sie einen Web-Data Vault-Server installieren, beginnen Sie nach dem Abrufen einer Lizenz vom Policy Server mit der Konfiguration des Web-Data Vault.

Geben Sie auf dem Bildschirm mit den Servereinstellungen den vollständig qualifizierten Domännennamen (FQDN) und den SSL-Port des Servers ein. Wenn Sie die Web-Data Vault-Richtlinie auf dem Policy Server konfigurieren, müssen Sie denselben FQDN verwenden. Der Name muss für alle Clientsysteme auflösbar sein, anderenfalls können bestimmte Systeme nicht in den Data Vaults auf diesem Server gesichert werden.

6. Wählen Sie auf dem Bildschirm mit den Zertifikateinstellungen zwischen folgenden Optionen:
 - Importieren eines bestehenden SSL-Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben wurde. Diese Option wird empfohlen und bietet die höchste Sicherheitsstufe.
 - Erstellen eines selbstsignierten SSL-Zertifikats. Diese Option bietet eine niedrigere Sicherheitsstufe und sollte nur zu Bewertungszwecken verwendet werden.

HINWEIS: Sie können das Zertifikat auf dem Web-Data Vault-Server jederzeit nach der Installation mit dem Dienstprogramm `DvConfig` austauschen. Dabei müssen Sie eine Installation mit einem selbstsignierten Zertifikat so umkonfigurieren, dass ein importiertes Zertifikat verwendet wird. Siehe „[Optionen für Web-Data Vaults über die Befehlszeilenschnittstelle \(DvConfig\) konfigurieren](#)“ (Seite 21).

7. Auf dem nächsten Bildschirm werden Sie aufgefordert, Namen für zwei Arten von Benutzern des Web-Data Vault-Servers anzugeben:
- **Benutzer mit Administratorrechten**, der sich um administrative Aufgaben wie das Erstellen und Löschen von Data Vaults sowie die Migration von Client-Sicherungsdaten kümmert.
 - **Benutzer mit Sicherungsrechten**, der Endbenutzervorgänge wie das Sichern und Wiederherstellen von Dateien durchführt.

Diese Benutzer sind speziell im Web-Data Vault-Server von Data Protector for PCs zu finden. Wenn Sie Web-Data Vaults für diesen Server erstellen oder bearbeiten, müssen Sie die Daten zu beiden Benutzern angeben.

HINWEIS: Passwörter müssen mindestens 8 Zeichen umfassen.

8. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**, um die Installation und Konfiguration des Web-Data Vault-Servers sowie die Installation der Cleanup-Software abzuschließen.

Verwalten der Web-Data Vaults

1. Geben Sie auf der Seite mit den Data Vault-Richtlinien den vollständig qualifizierten Domänennamen und SSL-Port des Servers an sowie die Anmeldeinformationen des Kontos für den Benutzer mit Sicherungsrechten. Klicken Sie dann auf **Data Vaults konfigurieren**.
2. Übermitteln Sie die Anmeldeinformationen des Kontos für den Benutzer mit Administratorrechten. Die Seite für die Verwaltung des Web-Data Vault-Servers wird angezeigt.

Hier können Sie vorhandene Web-Data Vaults auswählen oder löschen. Sie können auch einen neuen Data Vault hinzufügen.

HINWEIS: Sie können einen vorhandenen Data Vault nur dann auswählen, wenn sich auf diesen aktuell keine andere Data Vault-Richtlinie bezieht.

3. Stellen Sie sicher, dass Sie die Data Vault-Richtlinie speichern, indem Sie unten auf der Seite auf **Speichern** klicken.
4. Wenn Sie einen neuen Data Vault hinzugefügt haben, können Sie testen, ob der Data Vault vorhanden ist und die gewünschte Konfiguration aufweist.

Migrieren von Daten eines Data Vaults in einer Windows-Dateifreigabe in einen Web-Data Vault

Das Layout von Daten in einem Data Vault ist für in der Windows-Dateifreigabe gespeicherte Data Vaults und für HTTPS-basierte Web-Data Vaults identisch. Das bedeutet, dass Sie Daten von vorhandenen DPNE 6.x-Data Vaults in neue Web-Data Vaults migrieren können.

HINWEIS: Datenmigrationen können nur für Data Vaults durchgeführt werden, die demselben Policy Server zugeordnet sind oder dasselbe Verschlüsselungspasswort aufweisen.

Es gibt zwei mögliche Szenarien für die Datenmigration:

- Verwenden desselben Systems, um den Web-Data Vault zu hosten.

HINWEIS: Paralleles Zugreifen auf das gleiche Verzeichnis über eine Windows-Dateifreigabe und einen Web-Data Vault wird nicht unterstützt.

- Verschieben des gesamten Data Vaults auf ein anderes System.

In beiden Fällen muss der Web-Data Vault-Server lokal auf dem für die Daten vorgesehene System installiert sein.

So migrieren Sie Daten eines vorhandenen Data Vaults in einer Windows-Dateifreigabe in ein Web-Data Vault:

HINWEIS:

- Führen Sie die Migration außerhalb der Arbeitszeit durch, um die Auswirkungen auf Sicherungen zu minimieren, die gerade durchgeführt werden.
 - Stellen Sie mithilfe des Task-Managers von Windows sicher, dass `DPNECleanup.exe` nicht ausgeführt wird.
 - Überprüfen Sie die Cleanup-Richtlinie auf dem Policy Server, um sicherzustellen, dass die Ausführung von `DPNECleanup.exe` nicht während der Migrationsphase geplant ist.
-

1. Installieren Sie den Web-Data Vault-Server und aktualisieren Sie den Policy Server und die Agenten auf Version 7.0. Stellen Sie sicher, dass alle Agenten nach der Installation der Version 7.0 neu gestartet wurden, da nur dann die Sicherung von Daten auf dem Web-Data Vault erfolgen kann.
2. Deaktivieren Sie die entsprechende Richtlinie für die Windows-Dateifreigabe auf der Seite mit den Data Vault-Richtlinien, sodass die Agenten das Kopieren der Daten in den Data Vault einstellen.
3. Wenn Sie dasselbe Verzeichnis für den Web-Data Vault verwenden möchten, beenden Sie die Freigabe des Verzeichnisses via CIFS.

4. Wenn sich der Web-Data Vault auf einem anderen Server als der Data Vault in der Windows-Dateifreigabe befindet, müssen die Daten auf diesen Computer unter Verwendung eines Ordnerpfads kopiert werden, der nicht mehr als 67 Zeichen aufweist. Wenn sich der Data Vault auf demselben Server befindet, müssen keine Daten an einen neuen Speicherort kopiert werden, sofern dies nicht aus anderen Gründen erforderlich ist.
5. Vor dem Erstellen des neuen Web-Data Vaults müssen Sie entscheiden, wie der Anfangsaktualisierungsprozess ablaufen soll. Die Anfangsaktualisierung kann übersprungen werden, wenn für alle Agenten eine Anfangsaktualisierung durchgeführt wurde, sodass sich bereits sämtliche Sicherungsdaten im vorhandenen Data Vault befinden. Die Option zum Überspringen der Anfangsaktualisierung ist nicht unmittelbar Teil einer Data Vault-Richtlinie, jedoch Teil der Kopierrichtlinie, auf die verwiesen wird. Stellen Sie sicher, dass eine Data Vault-Richtlinie mit entsprechend ausgewählten Optionen vorhanden ist (d. h. mit deaktivierter Option für die Anfangsaktualisierung und geeigneten Einstellungen für Drosselung und Zeitplanung). Erstellen Sie eine neue Kopierrichtlinie dafür oder bearbeiten Sie eine vorhandene Richtlinie (in diesem Fall wirken sich die Änderungen auf alle Data Vault-Richtlinien aus, die auf die Kopierrichtlinie verweisen).
6. Erstellen und speichern Sie die neue Data Vault-Richtlinie für den Web-Data Vault. Wenn Sie einen neuen Web-Data Vault erstellen, müssen Sie den Ordnerpfad angeben. In diesem Fall handelt es sich um den Pfad zu dem Speicherort, an dem sich die eigentlichen von Ihnen zu migrierenden Daten des Data Vaults in der Windows-Dateifreigabe befinden. Wählen Sie die von Ihnen in Schritt 5 erstellte Kopierrichtlinie aus. Legen Sie die anderen Optionen für die Data Vault-Richtlinie entsprechend der Optionen der ursprünglichen Richtlinie für die Windows-Dateifreigabe fest (beispielsweise die Netzwerkeinstellungen und Active Directory-Einstellungen).
7. Sobald Sie überprüft haben, dass die Agenten erfolgreich Dateien in den neuen Web-Data Vault sichern, löschen Sie die ursprüngliche Richtlinie für die Windows-Dateifreigabe.

Nach dem Sie die Richtlinie gespeichert haben, fahren die Agenten mit dem Kopieren der Daten in den neuen Web-Data Vault mithilfe des HTTPS-Protokolls fort.

Optionen für Web-Data Vaults über die Befehlszeilenschnittstelle (DvConfig) konfigurieren

Durch die Verwendung dieses Dienstprogramms über die Befehlszeilenschnittstelle können Sie die Konfigurationsparameter eines Web-Data Vaults ändern, beispielsweise Benutzer mit Sicherungsrechten und Benutzer mit Administratorrechten sowie deren Passwörter. Außerdem können Sie ein neues Zertifikat importieren, die SSL-Einstellung ändern und ein selbstsigniertes Zertifikat erstellen.

Bevor Sie Änderungen an den Parametern vornehmen, müssen Sie den Web-Data Vault-Server anhalten, indem Sie den vom Windows-Dienstprozess ausgeführten Data Vault-Server mit HP Data Protector for PCs anhalten.

Starten Sie den Web-Data Vault-Dienst neu, nachdem Sie Änderungen vorgenommen haben. Aktualisierungen der Richtlinien werden an die Agents verteilt.

HINWEIS: Wenn Sie `DvConfig` verwenden, um den SSL-Port oder den Namen oder das Passwort des Benutzers mit Sicherungsrechten auf dem Web-Data Vault-Server zu ändern, stellen Sie sicher, dass Sie die jeweiligen Data Vault-Richtlinien auf dem Policy Server entsprechend ändern.

Verwendung:

```
DvConfig [-adminUser Anmeldename:Passwort -backupUser  
Anmeldename:Passwort] [-h] [-i Zertifikatsdatei | -s Hostname]  
[-p Port] [-v]
```

`-adminUser Anmeldename:Passwort`

Festlegen der Anmeldedaten für das DvAdmin-Konto. Wird kein Anmeldename oder Passwort angegeben, wird der Standardbenutzer „DvAdmin“ verwendet.

`-backupUser Anmeldename:Passwort`

Festlegen der Anmeldedaten für das DvBackup-Konto. Wird kein Anmeldename oder Passwort angegeben, wird der Standardbenutzer „DvBackup“ verwendet.

`-h`

Drucken dieser Meldung.

`-i certfile`

Importieren eines vorhandenen Zertifikats.

`-p Port`Festlegen des SSL-Ports.

`-s Hostname`

Erstellen eines selbstsignierten Zertifikats für den vollständig qualifizierten Domännennamen.

`-v`

Drucken der Versionsinformationen und Beenden.

4 Data Protector for PCs-Schutzrichtlinien konfigurieren

Ersteinrichtung nach der Installation von Data Protector for PCs

Direkt nach der Installation von Data Protector for PCs wird das Fenster für die Ersteinrichtung in der Policy Server Console angezeigt. Bevor Sie Richtlinien für Data Protector for PCs festlegen können, müssen Sie zwei Konfigurationsschritte erfolgreich abschließen:

1. Definieren oder importieren Sie ein Verschlüsselungspasswort.

Aus Sicherheitsgründen müssen Sie ein Verschlüsselungspasswort definieren, bevor Sie Data Protector for PCs verwenden können. Damit wird sichergestellt, dass alle Dateien auf dem Benutzercomputer verschlüsselt werden und verschlüsselt über das Netzwerk übertragen werden. Es wird dasselbe Passwort verwendet, um die Dateien aller Benutzer und aller zentral konfigurierten Data Vaults zu verschlüsseln.

- Zentral (über die Policy Server Console) definierte Data Vaults verwenden zur Verschlüsselung immer das Data Protector for PCs-Verschlüsselungspasswort.
- Bei lokal (von Benutzern über deren Computer) definierten Data Vaults können die Benutzer jeweils auswählen, ob die Verschlüsselung verwendet werden soll, und eigene Passwörter festlegen.

Bei der Erstinstallation von Data Protector for PCs müssen Sie ein Passwort **generieren** oder **importieren**, bevor Sie fortfahren können. Nach der Generierung eines Passworts sollten Sie dieses zur Sicherheit **exportieren**. Dabei wird es an einem gesicherten Speicherort gespeichert. Später können Sie es zum Importieren verwenden.

Klicken Sie auf **Verschlüsselungsrichtlinie festlegen**, um das Passwort zu verwalten, und befolgen Sie die angezeigten Anweisungen.

HINWEIS: Nachdem ein Passwort generiert oder importiert wurde, kann es nicht mehr geändert werden.

2. Lizenzieren Sie Data Protector for PCs.

Mit der Testversion von Data Protector for PCs können Sie 60 Tage lang ohne Lizenz eine beliebige Anzahl von Benutzern schützen. Wenn Sie Data Protector for PCs kaufen, müssen Sie über den HP License Key Delivery Service unter <https://webware.hp.com/welcome.asp> einen Lizenzschlüssel herunterladen, den Sie anschließend eingeben. Sie können die folgenden Lizenzen kaufen:

- TA032AA oder TA032AAE für 100 Agenten
- TA033AA oder TA033AAE für 1000 Agenten
- TA036AA oder TA036AAE für 100 Agenten und HP Data Protector Starter Pack Windows (B6961BA oder B6961BAE)

Sie müssen vor dem Ende der Testperiode einen dauerhaft gültigen Lizenzschlüssel eingeben. Andernfalls können die Agenten nach Ablauf der 60 Tage keine Daten mehr in die Local Repositories oder Data Vaults kopieren. Allerdings können zuvor geschützte Dateiversionen immer noch wiederhergestellt werden.

Klicken Sie auf **Lizenzverwaltung**, um die Lizenzen zu verwalten, und anschließend auf **Geben Sie einen Lizenzschlüssel für Benutzer von Data Protector for PCs ein**. Befolgen Sie die angezeigten Anweisungen.

HINWEIS: Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Nachdem Sie diese Konfigurationsschritte erfolgreich abgeschlossen haben, steht Ihnen der volle Funktionsumfang der Policy Server Console zur Verfügung. Wenn Sie Data Protector for PCs soeben erst installiert haben, konfigurieren Sie die weiteren Elemente von Data Protector for PCs in der im nächsten Abschnitt angegebenen Reihenfolge.

Erstkonfiguration

In Data Protector for PCs sind verschiedene Richtlinien vorkonfiguriert, die für die meisten Organisationen ausreichen. Es wird empfohlen, zuerst Data Vault-, Kopier- und Dateischutzrichtlinien zu konfigurieren und anschließend die Data Protector for PCs-Agentensoftware auf den Desktop-PCs und Notebooks der Benutzer zu installieren.

HINWEIS: Statt neue Richtlinien zu konfigurieren, können Sie auch die vorkonfigurierten Richtlinien von Data Protector for PCs ändern. Wählen Sie dazu in den einzelnen Schritten jeweils **Vorhandene Richtlinie bearbeiten** statt **Neue Richtlinie erstellen** aus.

Die Schutzrichtlinien für Ihre Installation konfigurieren Sie über die Policy Server Console. Die von Ihnen zentral definierten Richtlinien werden an alle Data Protector for PCs-Agenten verteilt und auf den Desktop-PCs und Notebooks der Benutzer ausgeführt.

1. Sie können die Policy Server Console von Data Protector for PCs nach Abschluss des Installationsassistenten ausführen oder zu jedem beliebigen anderen Zeitpunkt über die folgende URL im Browser aufrufen:

`http://PolicyServer/dpnepolicy/`

Dabei steht „*PolicyServer*“ für den Namen Ihres Data Protector for PCs-Policy Server. Sie müssen als „Administrator“ auf dem Server angemeldet sein.

2. **Konfigurieren Sie Data Vault-Richtlinien.**

Data Vault-Richtlinien legen das Speicherziel (einen Web-Data Vault oder eine Windows-Dateifreigabe) für die kontinuierliche Sicherung der Benutzerdateien fest, die durch Richtlinien geschützt sind. Wenn eine Datei geändert wird, können die Vorgängerversion und die geänderte Datei automatisch an einem oder mehreren Speicherzielen gesichert werden. Jeder Benutzergruppe können ein oder mehrere Data Vaults zugewiesen werden. Sie können beispielsweise eine Data Vault-Richtlinie

mit dem Namen *Sales* definieren und diese Ihren Benutzergruppen *Dallas.Sales*, *San Francisco.Sales*, *Chicago.Sales* und *Atlanta.Sales* zuweisen.

- Zentral (über die Policy Server Console) definierte Data Vaults verwenden zur Verschlüsselung immer das Verschlüsselungspasswort von Data Protector for PCs.
- Bei lokal (von Benutzern über deren Agentensoftware) definierten Data Vaults können die Benutzer jeweils auswählen, ob die Verschlüsselung verwendet werden soll, und eigene Passwörter festlegen.

HINWEIS: *Voraussetzung für alle Data Vaults:*

Data Protector for PCs legt für die auf dem Dateiserver gesicherten Dateien die gleichen Zugriffsberechtigungen (ACLs) fest, die auch für die Originaldatei gelten. Dies bedeutet, dass ein Benutzer gesicherte Dateien nur wiederherstellen kann, wenn er auf seinem Computer auf die Originaldateien zugreifen kann.

Voraussetzung für Data Vaults in Windows-Dateifreigaben:

Wenn Sie standardmäßige Data Vaults in Windows-Dateifreigaben verwenden, sollten sich die Freigaben auf einem Windows-Dateiserver befinden. Dieser muss nicht mit dem Computer identisch sein, auf dem sich der Policy Server befindet. Wenn Sie Data Protector for PCs jedoch nur mit einer kleinen Anzahl installierter Agenten testen, kann es sinnvoll sein, für den Policy Server und den Data Vault-Dateiserver denselben Computer zu verwenden.

Gehen Sie wie folgt vor, um eine Data Vault-Richtlinie zu erstellen:

- a. Klicken Sie auf **Richtlinien > Data Vaults > Data Vault-Richtlinien** im Navigationsbereich auf der linken Seite.
- b. Klicken Sie auf **Neue Data Vault-Richtlinie erstellen**.
- c. Befolgen Sie die angezeigten Anweisungen. Die Prozesse für webbasierte Data Vaults und Data Vaults in einer Windows-Dateifreigabe unterscheiden sich.

HINWEIS: Wenn Sie einen Data Vault erstellen, darf der Pfad des Ordners oder der Freigabe nicht länger als 66 Zeichen sein.

Empfohlene Einstellungen:

Lassen Sie die Einstellung für die Kopierrichtlinie zunächst unverändert auf „Standard“.

Beachten Sie für Cleanups von Data Vaults in einer Windows-Dateifreigabe Folgendes:

- Wenn sich der Data Vault auf diesem Policy Server befindet, lassen Sie die Standardeinstellung für den Namen des Computers unverändert.

- Wenn sich der Data Vault auf einem anderen Windows-Dateiserver befindet, installieren Sie die Cleanup-Software für Data Vaults auf diesem Server, und geben Sie diesen Computer als Cleanup-Computer an.

3. Konfigurieren Sie Kopierichtlinien.

Eine Kopierichtlinie begrenzt die Anzahl der Clients, die gleichzeitig in einen Data Vault kopieren können. Außerdem werden in der Kopierichtlinie die Anfangsaktualisierung und der Zeitplan für die Data Vault-Aktualisierungen festgelegt, um die kontinuierliche Sicherung zu ergänzen. Jede Kopierichtlinie kann einem oder mehreren Data Vaults zugewiesen werden.

Kopierichtlinien definieren Folgendes:

- Anzahl der Agenten, die gleichzeitig Dateien auf Ihre Data Vaults kopieren können.
- Ein Zeitplan für regelmäßige Aktualisierungen, bei denen geprüft wird, ob alle erwarteten Dateien für einen Benutzer im Data Vault vorhanden sind. Ist dies nicht der Fall, werden die fehlenden Dateien kopiert. Damit wird noch einmal sichergestellt, dass alle Benutzerdateien ordnungsgemäß auf den Data Vault kopiert wurden.
- Ob eine **Anfangsaktualisierung** (oder -kopie) durchgeführt werden soll. Die Anfangsaktualisierung wird benötigt, da während des normalen Betriebs von Data Protector for PCs nur Informationen über die Änderungen in den Data Vault kopiert werden, wenn ein Benutzer eine von Data Protector for PCs im Continuous-Modus geschützte Datei ändert.

Die Standard-Kopierichtlinie gilt für alle Data Vaults, für die keine eigenen Kopierichtlinien festgelegt sind. Die Einstellungen der Standard-Kopierichtlinie können geändert werden, umbenannt oder gelöscht werden kann sie jedoch nicht.

Gehen Sie wie folgt vor, um eine Kopierichtlinie zu erstellen:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Kopierichtlinien festlegen**.
- c. Klicken Sie auf **Neue Kopierichtlinie erstellen**.
- d. Befolgen Sie die angezeigten Anweisungen.

Empfohlene Einstellungen:

- **Drosseln:** Geben Sie als Zeitraum Ihre normalen Geschäftszeiten an, und legen Sie für andere Zeiten eine geringere Drosselungsgrenze fest.
- **Anfangsaktualisierung:** Aktivieren Sie die Anfangsaktualisierung, um sicherzustellen, dass alle gemäß den Dateischutzrichtlinien geschützten Benutzerdateien gesichert werden.
- **Dateien wöchentlich/monatlich aktualisieren:** Da eine Aktualisierung nur wenige oder gar keine Dateikopiervorgänge beinhalten sollte, aktivieren Sie die Data

Vault-Aktualisierungen, um sicherzustellen, dass alle durch Richtlinien geschützten Benutzerdateien ordnungsgemäß gesichert werden.

4. Konfigurieren Sie Dateischutzrichtlinien.

Mit Dateischutzrichtlinien können Sie angeben, welche Dateien geschützt werden und wie lang Vorgängerversionen aufbewahrt werden sollen. Sie können beispielsweise eine Dateischutzrichtlinie mit dem Namen *Office-Dokumente* für Word-Dokumente, Excel-Dateien und PowerPoint-Präsentationen definieren.

Auf lokalen Festplatten gespeicherte Dateien können geschützt werden.

Es gibt zwei verschiedene Typen von Richtlinien:

- **Continuous File Protection** – bietet Echtzeitschutz für Dateien bei jedem Speichern oder Löschen. Im Allgemeinen sollten alle Dateien oder Dokumente, bei denen Sie über ein Menü die Option **Speichern** auswählen können, mit einer Continuous File Protection-Richtlinie geschützt werden.

Data Protector for PCs enthält mehrere Beispielrichtlinien. Drei davon sind nach der Installation standardmäßig ausgewählt: *Office-Dokumente*, *Softwareentwicklung* und *Webdokumente*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

- **Open File Protection** – schützt die Dateien, indem in regelmäßigen Abständen (meistens einmal pro Stunde) eine „Momentaufnahme“ von der Datei gemacht wird. Normalerweise sollte jede Datei, die entweder sehr groß ist (über 100 MB), die den größten Teil des Tages geöffnet ist oder die nicht über ein Menü mit der Option **Speichern** verfügt, mit diesem Verfahren geschützt werden. Häufig vorkommende Dateien dieses Typs sind E-Mail- und Datenbankdateien.

In Data Protector for PCs sind dazu vier Beispiele vorhanden: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* und *Thunderbird*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

HINWEIS: Data Protector for PCs unterstützt nicht die Sicherung von mit EFS verschlüsselten Dateien mit Open File Protection-Richtlinien. Daher dürfen beispielsweise .pst-Dateien nicht mit EFS verschlüsselt sein.

Gehen Sie wie folgt vor, um eine Dateischutzrichtlinie zu erstellen:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Dateischutzrichtlinien festlegen**.
- c. Klicken Sie entweder auf **Neue Continuous File Protection-Richtlinie erstellen** oder auf **Neue Open File Protection-Richtlinie erstellen**.
- d. Befolgen Sie die angezeigten Anweisungen.

HINWEIS: Achten Sie beim Erstellen von Dateischutzrichtlinien und beim Festlegen von Ausschluss- und Einschlussregeln darauf, dass Dateierweiterungen bei den Richtlinien für Open File Protection nicht länger als 9 Zeichen und bei den Richtlinien für Continuous File Protection nicht länger als 29 Zeichen sein dürfen.

Bei Open File Protection-Richtlinien können Sie für Einschlussregeln auch Dateien ohne Erweiterung auswählen. Bei Continuous File Protection-Richtlinien ist dies nicht möglich.

- ① **WICHTIG:** Sie haben nun alle grundlegenden Richtlinien konfiguriert, die Data Protector for PCs benötigt. In Data Protector for PCs sind noch weitere Richtlinien vorkonfiguriert, die für die meisten Organisationen ausreichen. Es wird empfohlen, zu diesem Zeitpunkt mit der Installation der Agenten auf den Desktop-PCs und Notebooks Ihrer Benutzer zu beginnen (siehe „[Data Protector for PCs-Agenten installieren](#)“ (Seite 37)). Später können Sie die restlichen Data Protector for PCs-Richtlinien prüfen und konfigurieren, z. B. die Cleanup-Richtlinie, die Benutzerkontrollrichtlinie, die Agentenaktualisierungsrichtlinie und die Richtlinie für den Berichtsdatenerhalt.
-

Weitere Richtlinien konfigurieren

1. Konfigurieren Sie den Active-Directory-Zugriff.

HINWEIS: *Zuordnung von Active-Directory-Gruppen zu Data Vaults:* In der Data Vault-Richtlinie können Sie Data Vaults zu Active-Directory-Gruppen zuordnen. Für alle Mitglieder der zugeordneten Gruppen erfolgt die Sicherung im zugeordneten Data Vault. Sie können keine einzelnen Benutzer zuordnen. Außerdem gilt, dass durch die Zuordnung einer Organisationseinheit nur die Gruppen innerhalb dieser Organisationseinheit zugeordnet werden. Alle Benutzer, die sich direkt in der Organisationseinheit befinden, werden dem Data Vault nicht zugeordnet. In der Liste der Active-Directory-Gruppen können sich fälschlicherweise andere Gruppen als Sicherheitsgruppen befinden, z. B. Verteilungsgruppen. Dem Data Vault werden jedoch nur Sicherheitsgruppen zugeordnet.

Mehrere Benutzer: Wenn zwei oder mehr Benutzer einen Computer gemeinsam nutzen, müssen sie zu derselben Active-Directory-Gruppe gehören.

Wenn Sie Data Vaults bestimmten Gruppen oder Organisationseinheiten zuweisen oder Berichte für bestimmte Gruppen oder Organisationseinheiten erstellen möchten, müssen Sie den Policy Server so konfigurieren, dass er auf Ihr Active Directory zugreifen kann.

Durch das Konfigurieren des Active-Directory-Zugriffs wird die Option **Mitglieder von Gruppen und Organisationseinheiten** für Data Vaults aktiviert (siehe „[Erstkonfiguration](#)“ (Seite 24)).

Gehen Sie wie folgt vor, um den Active-Directory-Zugriff zu konfigurieren:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Konfiguration**.
- b. Klicken Sie auf **Active-Directory-Zugriff konfigurieren**.
- c. Befolgen Sie die angezeigten Anweisungen.

2. Konfigurieren Sie die Cleanup-Richtlinie.

Für die Local Repositories von Data Protector for PCs auf den Benutzercomputern und die Data Vaults auf den Data Vault-Servern muss regelmäßig ein Cleanup durchgeführt werden, um Versionen zu entfernen, die gemäß den in den Dateischutzrichtlinien definierten Dateierhalteinstellungen zu alt sind.

Gehen Sie wie folgt vor, um die Cleanup-Richtlinie zu konfigurieren:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Cleanup-Richtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

Damit der Data Vault mehr Benutzer unterstützen kann, führen Sie den Cleanup-Prozess nur an Wochenenden (ab Freitagabend oder Samstagmorgen) aus. Dadurch steht für die Ausführung die maximale Zeit zur Verfügung:

- a. Öffnen Sie in der Policy Server Console die Seite **Cleanup-Richtlinie**, und ändern Sie den Eintrag **Cleanup-Zeitplan für Data Vault**.
- b. Entfernen Sie die Markierung für alle Tage außer Freitag oder Samstag:
 - Für Freitag wählen Sie eine Startzeit am späten Abend, wie z. B. 22 Uhr.
 - Für Samstag wählen Sie eine Startzeit am frühen Morgen, wie z. B. 1 Uhr.

Wenn das Cleanup nur an Wochenenden durchgeführt wird:

- Die Liste der Dateien, die für die Wiederherstellung aus einem Data Vault angezeigt wird, kann bis zu einer Woche veraltet sein. Benutzer können jederzeit eine manuelle neue Prüfung ihrer Daten im Data Vault durchführen, um die Anzeige zu aktualisieren.
- Sicherungsversionen bleiben bis zu einer Woche länger erhalten, weil das Cleanup nur an Wochenenden ausgeführt wird.
- Die Kontingentverwaltung ist nicht auf dem aktuellen Stand. Wenn Benutzer ihr Kontingent überschreiten, müssen sie möglicherweise bis zur Cleanup-Ausführung warten, damit im Data Vault wieder Speicherplatz verfügbar ist. Andererseits wird eine Überschreitung des Kontingents im System möglicherweise nicht sofort erkannt, da die Berichte zur Speicherplatzauslastung im Rahmen des Cleanup-Prozesses erstellt werden.

Empfohlene Einstellungen:

- **Cleanup-Zeitplan für Local Repository:** Lassen Sie die Standardeinstellung (1 Stunde) unverändert.
- **Cleanup-Zeitplan für Data Vault:** Die Standardeinstellung (Cleanup täglich um Mitternacht) sollte für die meisten Installationen geeignet sein. Unter

„Sizing-Empfehlungen“ (Seite 32) finden Sie weitere Informationen zur Data Vault-Kapazität.

- Sie können DPNECleanup so konfigurieren, dass mehrere Threads auf wiederverwendbare und erweiterbare Weise verwendet werden, um die CPU und die Festplatte besser zu nutzen und damit die Speicherung größerer Datenmengen zu ermöglichen. Siehe „Konfigurieren des Multithread-Cleanup“ (Seite 35).

3. Konfigurieren Sie die Benutzerkontrollrichtlinie.

Die Benutzerkontrollrichtlinie bestimmt, wie viel Kontrolle die Benutzer über die an ihre Computer verteilten Unternehmensrichtlinien haben.

Gehen Sie wie folgt vor, um die Benutzerkontrollrichtlinie zu konfigurieren:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Benutzerkontrollrichtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

Empfohlene Einstellungen:

Wählen Sie für **Wiederherstellung durch Benutzer** die Einstellung **Benutzerkontrolle zulassen** aus.

4. Konfigurieren Sie die Agentenaktualisierungsrichtlinie.

Die Richtlinie gibt an, welche Version des Data Protector for PCs-Agenten auf allen von Data Protector for PCs geschützten Desktop-PCs und Notebooks verwendet werden soll. Der Agent wird automatisch auf diese Version aktualisiert.

Gehen Sie wie folgt vor, um die Agentenaktualisierungsrichtlinie zu konfigurieren:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Agentenaktualisierungsrichtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

5. Konfigurieren Sie den Berichtsdatenerhalt.

Damit wird für jede Hauptkategorie von Informationen festgelegt, wie lang die Daten für Berichtszwecke aufbewahrt werden sollen.

Gehen Sie wie folgt vor, um den Berichtsdatenerhalt zu konfigurieren:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Konfiguration**.
- b. Klicken Sie auf **Erhalt der Berichtsdaten konfigurieren**.
- c. Befolgen Sie die angezeigten Anweisungen.

Weitere Konfigurationsschritte

Diese Schritte werden normalerweise bei der Erstinstallation von Data Protector for PCs durchgeführt.

Lizenzieren Sie Ihre Data Protector for PCs-Software.

Mit der Testversion von Data Protector for PCs können Sie 60 Tage lang ohne Lizenz eine beliebige Anzahl von Benutzern schützen. Wenn Sie Data Protector for PCs kaufen, müssen Sie über den HP License Key Delivery Service unter <https://webware.hp.com/welcome.asp> einen Lizenzschlüssel herunterladen, den Sie anschließend eingeben.

Gehen Sie wie folgt vor, um einen Lizenzschlüssel einzugeben:

1. Klicken Sie im Navigationsbereich auf der linken Seite auf **Lizenzverwaltung**.
2. Klicken Sie auf **Geben Sie einen Lizenzschlüssel für Benutzer von HP Data Protector for PCs ein**.
3. Befolgen Sie die angezeigten Anweisungen.

Wenn Sie mehrere Lizenzen eingeben müssen, können Sie eine Textdatei mit einer Lizenzschlüsselzeichenfolge in jeder Zeile erstellen. Sie können die Datei dann über das Feld „Lizenzschlüssel importieren“ importieren.

HINWEIS: Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Lizenzen verschieben

Wenn Sie die IP-Adresse des Policy Server ändern müssen, um den Server in ein anderes System zu verschieben, oder wenn Sie Lizenzen von einem Policy Server zu einem anderen verschieben müssen, wenden Sie sich an den HP License Key Delivery Service unter <https://webware.hp.com/welcome.asp>.

Definieren, importieren und exportieren Sie ein Verschlüsselungspasswort.

Aus Sicherheitsgründen müssen Sie ein Verschlüsselungspasswort definieren, bevor Sie Data Protector for PCs verwenden können. Damit wird sichergestellt, dass alle Dateien auf dem Benutzercomputer verschlüsselt werden und verschlüsselt über das Netzwerk übertragen werden. Es wird dasselbe Passwort verwendet, um die Dateien aller Benutzer und aller zentral konfigurierten Data Vaults zu verschlüsseln.

- Zentral (über die Policy Server Console) definierte Data Vaults verwenden zur Verschlüsselung immer das Data Protector for PCs-Verschlüsselungspasswort.
- Bei lokal (von Benutzern über deren Computer) definierten Data Vaults können die Benutzer jeweils auswählen, ob die Verschlüsselung verwendet werden soll, und eigene Passwörter festlegen.

Bei der Erstinstallation von Data Protector for PCs müssen Sie ein Passwort generieren oder importieren, bevor Sie fortfahren können. Nach der Generierung eines Passworts sollten Sie dieses zur Sicherheit exportieren. Dabei wird es an einem gesicherten Speicherort gespeichert. Später können Sie es zum Importieren verwenden.

HINWEIS: Nachdem ein Passwort generiert oder importiert wurde, kann es nicht mehr geändert werden.

Gehen Sie wie folgt vor, um Ihr Verschlüsselungspasswort zu verwalten:

1. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.

2. Klicken Sie auf **Verschlüsselungsrichtlinie**.
3. Befolgen Sie die angezeigten Anweisungen.

Anzahl der Agents bestimmen, die unterstützt werden können

Es lassen sich nur schwer allgemeingültige Richtlinien für alle Umgebungen aufstellen. Daher wird in den hier angegebenen Fällen genau der Kontext beschrieben, für den die jeweiligen Zahlen gelten.

Einflussfaktoren beim Sizing

Das Sizing einer Data Protector for PCs-Umgebung gestaltet sich komplex. Zu den technischen Faktoren, die die Anzahl unterstützter Benutzer in einer bestimmten Umgebung beeinflussen können, zählen:

- Die Verarbeitungsleistung im Data Vault (für die nächtliche Konsolidierung der Sicherungsdaten)
- Die Netzwerk- und E/A-Bandbreite auf dem Data Vault-Server
- Der Festplattenplatz auf dem Data Vault-Server
- Die Größe der SQL-Datenbank auf dem Policy Server
- Die Netzwerkbandbreite und Verarbeitungsleistung auf dem Policy Server

Welche dieser Faktoren in einer bestimmten Installation zu Engpässen führen können, hängt sowohl von den Data Protector for PCs-Konfigurationseinstellungen als auch vom Verwendungsmuster ab:

- Anzahl der Benutzer auf einem Data Vault
- Anzahl und Größe der Dateien, die unter die konfigurierten Schutzrichtlinien fallen
- Änderungshäufigkeit der geschützten Dateien
- Einstellungen für den Erhalt geschützter Dateitypen

Sizing-Empfehlungen

Data Vault

Durch einen Zeitplan für tägliche Cleanups kann ein Data Vault mit 14 TB Speicherplatz eine Benutzerzahl von bis zu **3.500** Agenten unterstützen, wenn folgende durchschnittliche Datenmerkmale gelten:

- Durchschnittliche Anzahl der geschützten Dateien: 5000
- Durchschnittliche Gesamtgröße der geschützten Dateien auf der lokalen Festplatte: 10 GB
- Durchschnittliche Gesamtgröße im Data Vault (komprimiert): 4 GB

Wenn Sie durchschnittlich mehr Daten als in diesem Beispiel schützen müssen, schafft das Hinzufügen von Festplattenkapazität für den Data Vault zwar mehr Datenspeicherplatz, aber die nächtliche Konsolidierung der Sicherungsdaten im Data Vault kann möglicherweise nicht mehr zeitgerecht abgeschlossen werden. In diesem Fall haben Sie folgende Möglichkeiten:

- Führen Sie das Data Vault-Cleanup nur an Wochenenden aus. Weitere Informationen, wie Sie dabei vorgehen müssen, finden Sie unter „[Weitere Richtlinien konfigurieren](#)“ (Seite 28) in Schritt 2 (Cleanup-Richtlinie konfigurieren). Dadurch steigt die Anzahl der Agenten, die ein Data Vault mit 40 TB Speicherplatz und denselben durchschnittlichen Datenmerkmalen unterstützen kann, auf 10.000.
- Sie können Endbenutzerdaten über mehrere Data Vaults verteilen.

Die Hardwarespezifikationen für solche Data Vaults lauten wie folgt:

Data Vault-Typ	Tägliches Cleanup (bis zu 3.500 Agenten)	Wöchentliches Cleanup(bis zu 10.000 Agenten)
Windows-Dateifreigabe	3 GHz Dual Core, 4 GB RAM, 14 TB Speicherplatz	3 GHz Dual Core, 4 GB RAM, 40 TB Speicherplatz
Web-Data Vault	3 GHz Quad Core, 4 GB RAM, 14 TB Speicherplatz	3 GHz Quad Core, 4 GB RAM, 40 TB Speicherplatz

Wenn Ihre Benutzer durchschnittlich weniger Daten besitzen, können Sie eventuell eine höhere Benutzerzahl auf einem Data Vault unterbringen.

HINWEIS: HP empfiehlt dringend, dass sich das Betriebssystem des Data Vault und die Sicherungsdaten auf physisch getrennten Festplatten befinden sollten, um die Leistung zu optimieren.

Für eine optimale Leistung sollten Sie die Data Vault-Festplatte regelmäßig defragmentieren.

Richtlinienserver

Die Datenverkehrsmenge, die auf dem Policy Server erzeugt wird, hängt direkt von der Anzahl der Agents dieses Servers ab. Für die MS SQL Server Express Edition, die mit Data Protector for PCs bereitgestellt wird, gilt eine maximale Datenbankgröße von 4 GB, und es können nicht mehr als 5.000 Agenten¹ unterstützt werden.

Wenn Sie in Ihrer Umgebung mehr als 5.000 Agents unterstützen müssen, können Sie entweder weitere Policy Server hinzufügen oder MS SQL Express durch eine Vollversion von Microsoft SQL Server ersetzen. Auf diese Weise lässt sich der Policy Server problemlos auf bis zu 50.000 Agenten skalieren. Wenn Sie die Vollversion von MS SQL Server verwenden, sollten Sie eventuell den Hauptspeicher des Policy Server auf mindestens 3 GB aufrüsten.

1. Mit der Standardeinstellung von 30 Tagen für den Berichtsdatenerhalt auf dem Policy Server.

Für eine bessere Leistung sollte der Policy Server auf einem anderen Server als der Data Vault-Server ausgeführt werden. Beide Anwendungen können auf demselben Server ausgeführt werden, dies ist jedoch nur zu Bewertungszwecken ratsam.

Sie müssen mindestens einen Policy Server verwenden, aber die Anzahl der Data Vaults und Policy Server muss nicht übereinstimmen.

Netzwerkfaktoren

HINWEIS: Web-Data Vaults sind nicht von hoher Latenz betroffen. Folgende Informationen gelten nur für Data Vaults in Windows-Dateifreigaben.

HP empfiehlt bei Data Vaults in Windows-Dateifreigaben im Allgemeinen keine Anfangsaktualisierung von Data Protector for PCs-Agenten auf Data Vaults, wenn die Netzwerklatenz zwischen den beiden größer als 50 ms ist. Dies gilt in der Regel für Home-Offices oder Remote-Niederlassungen mit langsamer WAN-Verbindung. Die Anfangsaktualisierung kann zwar ausgeführt werden, dauert aber sehr lange.

Wenn Ihre Umgebung verschiedene Standorte umfasst und die Netzwerklatenz für manche davon größer als 50 ms ist, sollten Sie Data Vaults an mehreren Standorten installieren, damit alle Niederlassungen mindestens einen Data Vault mit einer Latenz von maximal 50 ms erreichen können.

Nachdem die Anfangsaktualisierung abgeschlossen ist, können Aktualisierungen von beliebigen Standorten in Ihrem Unternehmensnetzwerk oder sogar von einem Home-Office aus vorgenommen werden. Diese Aktualisierungen sind meist so klein, dass sie auch über langsame Netzwerkverbindungen gut funktionieren.

Wenn die Anfangsaktualisierung über eine Verbindung mit hoher Latenz durchgeführt werden muss, kann dies mehrere Tage dauern, doch der Vorgang lässt sich problemlos unterbrechen. Data Protector for PCs setzt die Aktualisierung an dem Punkt fort, an dem sie angehalten wurde, sobald wieder eine Verbindung zum Data Vault besteht.



TIPP: Wenn Sie die Latenz zwischen Ihren Standorten nicht kennen, setzen Sie von einem Computer an einem Standort einen ping-Befehl an einen Computer an einem anderen Standort ab. Durch jedes erfolgreiche Pingsignal können Sie die Latenz ermitteln.

5 Konfigurieren des Multithread-Cleanup

Die Leistung von DPNECleanup begrenzt die Menge der Benutzerdaten, die in einem Data Vault gesichert werden können. Sie können das DPNE-Cleanup so konfigurieren, dass mehrere Threads auf wiederverwendbare und erweiterbare Weise verwendet werden, um die CPU und die Festplatte besser zu nutzen und damit die Speicherung größerer Datenmengen zu ermöglichen.

Beim Multithread-Cleanup führt das Scheduler-Argument '-s' zu den Standardargumenten '-e -f -u -p -d 1000', einschließlich standardmäßigem Multithread-Cleanup und einer Verzögerung von 1 Sekunde für den Auto-Adjuster. Wenn Sie diese Standardeinstellungen nicht verwenden möchten, z. B. um die Multithread-Ausführung zu deaktivieren oder genauer einzustellen, löschen Sie das Argument '-s' aus dem Scheduler-Aufruf, und hängen Sie die einzelnen Befehlszeilenargumente an.

HINWEIS:

Auch wenn Sie das Multithread-Cleanup unter bestimmten Voraussetzungen deaktivieren möchten, sollten Sie '-e -f -u' als Argumente für den Cleanup-Aufruf im Data Vault beibehalten.

DPNECleanup.exe über die Befehlszeilenschnittstelle verwenden

Durch das Argument -p für DPNECleanup.exe kann das Cleanup initialisiert und die Parallel Engine gestartet werden, um eine Multithread-Ausführung zu ermöglichen. Die Parallel Engine bietet sieben optionale Befehlszeilenargumente. Die ausführbare Datei von DPNECleanup kann diese Argumente abrufen und an die Parallel Engine weiterleiten.

Ohne Angabe von -p wird DPNECleanup im seriellen Modus ausgeführt. In diesem Modus wird die Parallel Engine nicht verwendet.

dpnecleanup

-a *Affinität*

Setzt die Prozessoraffinität auf die angegebene Zahl, die für die festgelegten Bits der CPU-Kerne für die Threads steht.

-d *Verzögerung*

Legt die Verzögerung in Millisekunden fest, bevor der Auto-Adjuster eingreift, sodass die Parallel Engine genug Zeit erhält, eine Reihe von Threads zu starten und eine gewisse Systemauslastung zu erzeugen. In der Standardeinstellung bewirkt das Argument -s eine Verzögerung von 1000 Millisekunden bzw. 1 Sekunde.

-m *max_CPU_Auslastung*

Legt die gewünschte maximale CPU-Auslastung (für alle über Affinität definierten Kerne) auf *max_CPU_Auslastung* in % fest, die der Auto-Adjuster zu erreichen versucht. Für *max_CPU_Auslastung* muss eine Ganzzahl zwischen 1 und 100 angegeben werden. Die Standardeinstellung „0“ steht für unbegrenzt (volle CPU-Auslastung).

-o

Konstante Ressourcen, d. h., der Auto-Adjuster ist deaktiviert, und die Parallel Engine ändert nicht die Anzahl an gleichzeitigen Threads. Verwenden Sie -r, um die Anzahl an gleichzeitigen Threads anzupassen. Die Argumente -d, -m und -q werden bei der Ausführung mit -o ignoriert.

-p

Ermöglicht Multithread-Cleanup.

-q *max_Warteschlangenlänge*

Legt die gewünschte maximale durchschnittliche Länge der Warteschlange für die Festplatte fest, die der Auto-Adjuster zu erreichen versucht. Der Wert muss eine Gleitkommazahl sein. Die Standardeinstellung lautet „2.0“.

-r *Ressourcenzahl*

Legt die Anzahl der gleichzeitigen Ressourcen (Threads) auf die angegebene Zahl fest. Standardmäßig und in Kombination mit der Option -o nutzt das System $2^{(\text{CPU-Anzahl})}$ gleichzeitige Threads. Wird der Auto-Adjuster ausgeführt, steht der angegebene Wert für die Höchstzahl der gleichzeitigen Ressourcen in Form von Threads. Die Standardeinstellung für die maximale Anzahl lautet „0“, d. h. unbegrenzt.

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

Legt die Prozesspriorität für alle Threads fest. Die Standardeinstellung lautet Normal.

-s

Server-Cleanup. Legt das Cleanup für alle Data Vaults fest (zentral oder vom Benutzer definiert). Wird bei Multithreading durch die Argumente -e -f -u -p -d 1000 ersetzt, wenn der Befehl ausgeführt wird.

-e

Enterprise-Cleanup. Legt das Cleanup für alle Data Vaults fest, die durch zentrale Richtlinien des Policy Server definiert sind.

-f

Schnelles Cleanup. Normalerweise wird das Agenten-Cleanup nur ausgeführt, wenn sich das System im Leerlauf befindet. Durch diese Option kann das Cleanup jederzeit gestartet werden.

-u

Benutzerdefiniertes Cleanup. Legt das Cleanup für alle lokalen Data Vaults fest, die durch lokale, vom Benutzer erstellte Richtlinien definiert sind.

6 Data Protector for PCs-Agenten installieren

HINWEIS: Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Es gibt zwei Möglichkeiten, Data Protector for PCs-Agenten zu installieren:

- Installation auf allen Benutzercomputern einzeln. Siehe „Data Protector for PCs-Agenten auf einzelnen Clientcomputern installieren“ (Seite 37).
- Unternehmensweite Bereitstellung über einen Dateiserver, auf den alle Clientcomputer zugreifen können. Siehe „Data Protector for PCs-Agents unternehmensweit bereitstellen“ (Seite 38).

Data Protector for PCs-Agenten auf einzelnen Clientcomputern installieren


Voraussetzungen

Data Protector for PCs-Agentensoftware kann auf Desktop-PCs und Notebooks von Benutzern mit Windows installiert werden. Informationen zu unterstützten Plattformen finden Sie in der Unterstützungsmatrix.

Sie müssen mit einem Konto mit Administratorrechten angemeldet sein.

Installationsprozedur

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Der Installationsassistent sollte automatisch gestartet werden. Andernfalls starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf **Data Protector for PCs-Agentensoftware installieren oder aktualisieren**. Wenn ein Dialogfeld zum Öffnen oder Speichern angezeigt wird, wählen Sie **Öffnen** (bzw. **Ausführen**) aus.
3. Wenn auf dem Benutzercomputer nicht Microsoft Windows Installer 3.1 oder eine neuere Version installiert ist, bietet der Assistent diese Installation an. Wenn das Dialogfeld für die Aktualisierung von Windows Installer angezeigt wird, klicken Sie auf **OK**, um die Installation zu starten.
4. Wenn auf dem Benutzercomputer nicht Microsoft .NET Framework 2.0 SP1 oder eine neuere Version installiert ist, bietet der Assistent diese Installation an. Wenn das Dialogfeld für die Installation von Microsoft .NET Framework 2.0 SP1 angezeigt wird, klicken Sie auf **OK**, um die Installation zu starten.
5. Der Assistent installiert den Data Protector for PCs-Agenten automatisch. Befolgen Sie die angezeigten Anweisungen. Während der Installation werden Sie aufgefordert, Informationen zum Policy Server einzugeben.

6. Wenn die Installation und die Konfiguration abgeschlossen sind, klicken Sie auf **Fertig stellen**. Falls auf dem Policy Server eine Open File Protection-Richtlinie definiert ist, werden Sie aufgefordert, Ihr System erneut zu starten.
In der Taskleiste sollte jetzt ein Data Protector for PCs-Symbol angezeigt werden (eines der folgenden Symbole, je nach Schutzstatus: ).
7. Testen Sie, ob der Data Protector for PCs-Agent ordnungsgemäß funktioniert:
 - a. Öffnen oder erstellen Sie eine Testdatei, wie z. B. ein Word-Dokument oder eine Excel-Datei, und legen Sie sie beispielsweise auf dem Desktop ab. Nehmen Sie einige Änderungen daran vor, und klicken Sie auf **Speichern**.
 - b. Klicken Sie auf dem Desktop, im Windows Explorer oder in einem Dialogfeld zum Öffnen einer Datei mit der rechten Maustaste auf die Testdatei. Im Menü, das daraufhin geöffnet wird, sollten drei Data Protector for PCs-Einträge angezeigt werden (**Dateien finden und wiederherstellen...**, **Version kopieren** und **Version öffnen mit XXX...**).
 - c. Wählen Sie **Version öffnen mit XXX...** aus. Daraufhin sollte eine Liste der Versionen des soeben erstellten oder bearbeiteten Dokuments, jeweils mit Zeitstempel versehen, angezeigt werden. Wenn Sie eine der Versionen auswählen, wird sie als schreibgeschütztes Dokument in der jeweiligen Anwendung geöffnet. Auf diese Weise stellt ein Benutzer eine frühere Version seiner Dokumente aus dem lokalen Data Protector for PCs-Repository wieder her.
8. Wiederholen Sie die Schritte 1 bis 8 für alle anderen Desktop-PCs und Laptops, die mit Data Protector for PCs geschützt werden sollen.

Data Protector for PCs-Agents unternehmensweit bereitstellen

Bei der Erstinstallation können Sie Data Protector for PCs-Agents mithilfe des Data Protector for PCs Agent Deployment Kit, das auf der Installations-CD-ROM enthalten ist, unternehmensweit bereitstellen.

HINWEIS: Sie können das Deployment Kit nicht auf Vista-PCs mit aktivierter Benutzerkontensteuerung verwenden. In diesem Fall müssen Sie die Benutzerkontensteuerung deaktivieren oder den Agenten interaktiv installieren.

In der im Folgenden beschriebenen Prozedur kopieren Sie das Data Protector for PCs Agent Deployment Kit, das sich unter *CD-ROM:\Agent* befindet, zunächst in ein Verzeichnis auf einem Dateiserver, auf das alle Benutzer zugreifen können. Anschließend erstellen Sie mithilfe von *SetupConfig.exe* in diesem Verzeichnis eine Parameterdatei. Abschließend richten Sie einen Mechanismus ein, um *StartInstall.exe* im gemeinsam genutzten Verzeichnis auf jedem Benutzercomputer auszuführen. Sie können beispielsweise ein Anmeldeskript verwenden. Dann können Sie Ihre Bereitstellung über den Agent-Bereitstellungsbericht in der Policy Server Console von Data Protector for PCs überwachen.

Inhalt des Kits

Das Data Protector for PCs Deployment Kit enthält die folgenden Komponenten:

SetupConfig.exe	Erstellt und bearbeitet die Initialisierungsdatei.
StartInstall.exe	Startet Setup.exe als privilegierter Benutzer.
Setup.exe	Installiert die erforderlichen Komponenten und DataProtectorNE.ini.
DataProtectorNE.msi	Windows Installer-Paket für Data Protector for PCs zur Installation der Agentensoftware.
DataProtectorNE64.msi	Windows Installer-Paket für Data Protector for PCs zur Installation der Agentensoftware auf 64-Bit-Computern.
DataProtectorNE*.*.mst	Windows Installer-Pakete für Data Protector for PCs zur Installation der lokalisierten Agentensoftware.
WindowsInstaller.exe	Aktualisiert Windows Installer (erforderlich für die .NET-Installation).
NetFx20SP1_x64.exe, NetFx20SP1_x86.exe	Installiert NET Framework 2.0 SP1.
Setup.ini	Konfigurationsparameterdatei für die Data Protector for PCs-Installation. Diese Datei wird mithilfe von SetupConfig.exe erstellt (siehe Schritt 4 unten).

Bereitstellungs- und Installationsprozedur

1. Kopieren Sie die Dateien im Verzeichnis „Agent“ der Verteilungs-CD-ROM in ein Verzeichnis, auf das alle Benutzer, die das Data Protector for PCs Agent Deployment Kit verwenden werden, zugreifen können. Dabei kann es sich beispielsweise um das Verzeichnis einer NetLogon-Freigabe handeln, z. B. \\IhrServer\DPNEDeploy.
2. Stellen Sie sicher, dass das neu erstellte Verzeichnis die oben aufgeführten Dateien enthält. Alle anderen Dateien können Sie löschen.
3. Öffnen Sie ein DOS-Befehlsfenster (cmd.exe), und wechseln Sie mit cd zu dem in Schritt 1 erstellten Verzeichnis.
4. Führen Sie SetupConfig.exe aus, um die Parameterdatei Setup.ini zu erstellen oder zu bearbeiten. Bei der ersten Ausführung von SetupConfig.exe müssen Sie Werte für alle Parameter eingeben. Anschließend können Sie SetupConfig.exe wiederholt ausführen, um Parameter zu ändern. Wenn Sie keine Parameter ändern möchten, drücken Sie einfach die **Eingabetaste**.

Die folgenden Parameter sind erforderlich:

- **UNC-Pfad zu den Installationspaketen** – der vollständige Pfad zum gemeinsam genutzten Verzeichnis, in das die Dateien in Schritt 1 kopiert wurden, z. B. \\IhrServer\DPNEDeploy.

- Der Name des **Data Protector for PCs-Policy Server**. Dabei kann es sich um einen NetBIOS-Namen wie `IHR_SERVER` oder um einen vollständig qualifizierten Domänennamen wie z. B. `IhrServer.IhrUnternehmen.com` handeln.
 - **Benutzername** – der Benutzername eines Benutzers mit Administratorrechten auf den Computern, die das Data Protector for PCs Agent Deployment Kit verwenden, z. B. ein Mitglied aus der Gruppe der Domänenadministratoren. Dabei handelt es sich in der Regel um einen vollständig qualifizierten Benutzernamen einschließlich der Domäne, z. B. `IHR_UNTERNEHMEN\JerryAdmin`.
 - **Passwort** – das zum Benutzernamen gehörende Passwort. Dieses müssen Sie zweimal eingeben, um es zu bestätigen.
5. Führen Sie auf dem Clientcomputer die Datei `StartInstall.exe` aus, z. B. `\\IhrServer\DPNEDeploy\StartInstall`. Dadurch wird die Datei `Setup.exe` im Hintergrund mit geringer Priorität ausgeführt. Dabei werden die Anmeldedaten (Benutzername und Passwort) verwendet, die in der Datei `Setup.ini` angegeben sind. Dies kann im Rahmen eines Anmeldeskripts erfolgen. Beachten Sie, dass Sie dies nicht in ein Startskript aufnehmen können, da das Computerkonto nicht über ausreichende Netzwerkrechte verfügt.
 6. `Setup.exe` bestimmt, ob Data Protector for PCs auf dem Clientcomputer unterstützt werden kann. Informationen zu unterstützten Windows-Plattformen finden Sie in der Unterstützungsmatrix.
 7. `Setup.exe` bestimmt, ob .NET Framework Version 2.0 SP1 installiert ist. Wenn dies nicht der Fall ist, wird es installiert. Danach muss der Computer möglicherweise erneut gestartet werden.
 8. `Setup.exe` bestimmt, ob Data Protector for PCs bereits installiert ist. Wenn dies nicht der Fall ist oder eine ältere Version installiert ist, wird Data Protector for PCs installiert.

HINWEIS:

Wenn in den Schritten 4 bis 7 Fehler auftreten, werden auf dem Data Protector for PCs-Policy Server und im Anwendungsereignisprotokoll auf dem lokalen Computer entsprechende Nachrichten protokolliert.

Sie können den Fortschritt der Agent-Bereitstellung wie folgt über die Policy Server Console von Data Protector for PCs überprüfen:

1. Melden Sie sich an der Policy Server Console von Data Protector for PCs an.

2. Wählen Sie im Navigationsbereich auf der linken Seite unter **Berichte** den Eintrag **Agent-Bereitstellung** aus.
Daraufhin wird eine Zusammenfassung des Fortschritts Ihrer Erstbereitstellung bis zu diesem Zeitpunkt angezeigt. Darin ist Folgendes enthalten:
 - Anzahl der Computer, bei denen die Bereitstellung erfolgreich **abgeschlossen** wurde.
 - Anzahl der Computer, bei denen die Bereitstellung gerade **in Bearbeitung** ist.
 - Anzahl der Computer, bei denen die Bereitstellung **fehlgeschlagen** ist.
3. Klicken Sie in der Spalte **Anzahl der Computer** auf eine Zahl, um eine Liste der Computer im ausgewählten Bereitstellungsstatus anzuzeigen.
Zu jedem Computer wird der aktuelle Status angezeigt. Wenn die Bereitstellung beispielsweise auf einem bestimmten Computer fehlgeschlagen ist, wird der aufgetretene Fehler in der Informationsspalte angezeigt. Zusätzliche Informationen zu einem Computer können Sie anzeigen, indem Sie auf seinen NETBIOS-Namen klicken.

7 Aktualisieren von Data Protector for PCs

Wenn Sie Data Protector for PCs von Version 6.x auf 7.0 aktualisieren, gehen Sie in der folgenden Reihenfolge vor:

1. Aktualisieren Sie den Policy Server auf 7.0. Siehe „[Policy Server aktualisieren](#)“ (Seite 42).
2. Installieren Sie den Web-Data Vault-Server. Weitere Informationen finden Sie unter „[Installieren, Konfigurieren und Verwalten des Web-Data Vault-Servers](#)“ (Seite 18).
3. Aktualisieren Sie die Agenten auf 7.0.

Sie können die Agenten entweder durch die manuelle Aktualisierung oder „im Hintergrund“ über die Agentenaktualisierungsrichtlinie aktualisieren. Weitere Informationen finden Sie unter „[Agenten aktualisieren](#)“ (Seite 42).

Policy Server aktualisieren

Sie können die vorhandene Installation eines Data Protector for PCs-Policy Server mithilfe der Standard-Installationsprozedur auf eine neuere Version aktualisieren. Alle vorhandenen Konfigurationen (z. B. Data Vault-Konfiguration, Lizenzierung usw.) sind in der neueren Version verfügbar.

Aktualisieren des Policy Server:

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf der Assistentenseite für die Installation von Data Protector for PCs auf **Policy Server installieren**, um die Aktualisierung zu starten.
3. Befolgen Sie die angezeigten Anweisungen.
4. Die Installationsprozedur erkennt eine vorhandene Installation des Policy Server und bietet eine Aktualisierung an.
5. Befolgen Sie die angezeigten Anweisungen.
6. Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**. Anschließend können Sie die Policy Server Console von Data Protector for PCs starten.

HINWEIS: Wenn Cleanup-Software auf dem Policy Server installiert ist, müssen Sie auch diese aktualisieren. Dies können Sie entweder manuell oder über die Agentenaktualisierungsrichtlinie durchführen.

Agenten aktualisieren

Wenn Sie die Version des Data Protector for PCs-Servers aktualisieren, funktionieren vorhandene Agenten, die die frühere Version von Data Protector for PCs verwenden,

genau wie zuvor. Sie können die Agenten entweder durch die manuelle Aktualisierung oder „im Hintergrund“ über die Agentenaktualisierungsrichtlinie aktualisieren.

HINWEIS: Nach der Aktualisierung müssen alle Agenten neu gestartet werden, damit die neuen Web-Data Vaults verwendet werden können. Diese werden durch Popup-Meldungen im Infobereich der Taskleiste sowie auf der Übersichtsregisterkarte der Data Protector for PCs-Zustandsanzeige auf den jeweiligen Computern dazu aufgefordert.

Agenten automatisch über die Agentenaktualisierungsrichtlinie aktualisieren

Agenten können mithilfe der Agentenaktualisierungsrichtlinie des Policy Server „im Hintergrund“ aktualisiert werden. Das Installationspaket wird automatisch für alle verbundenen Clients bereitgestellt, und die Aktualisierung wird vollständig automatisiert durchgeführt. Der Endbenutzer wird nicht durch Unterbrechungen beeinträchtigt.

1. Wählen Sie in der Policy Server Console die Optionen **Richtlinien > Agentenaktualisierungsrichtlinie** aus.
2. Wenn Sie Ihren Policy Server soeben erst aktualisiert haben, wurde durch die Installationsprozedur ein neues Agentenaktualisierungspaket hochgeladen. In der Policy Server Console ist diese neue Version noch nicht ausgewählt.
Wählen Sie die neue Agentenversion aus, um sie zur Verfügung zu stellen.
3. Durch Anpassen der Drosselung können Sie die maximal zulässige Anzahl von Aktualisierungen pro Minute einstellen.
4. Klicken Sie auf **Agentenaktualisierungsrichtlinie speichern**.
5. Nun werden Agenten automatisch auf die neueste Version aktualisiert. Cleanup-Agenten werden ebenfalls automatisch aktualisiert.

HINWEIS: Sie können den Fortschritt der Agentenaktualisierung über den Bericht zur Agentenbereitstellung überprüfen.

Manuelle Aktualisierung von Agenten

Sie können einen vorhandenen Data Protector for PCs-Agenten mit der Standard-Installationsprozedur auf eine neuere Version aktualisieren.

Bevor Sie den Agenten auf eine neuere Version aktualisieren, stellen Sie sicher, dass die Agentenversion mit der Version des Data Protector for PCs-Policy Server kompatibel ist.

1. Legen Sie die CD-ROM für die Installation von Data Protector for PCs ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der Installations-CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf der Assistentenseite für die Data Protector for PCs-Installation auf **Agent installieren**, um die Aktualisierung zu starten.
3. Befolgen Sie die angezeigten Anweisungen.

4. Die Installationsprozedur erkennt eine vorhandene Agenteninstallation und bietet eine Aktualisierung an.
5. Befolgen Sie die angezeigten Anweisungen.

8 Support für Data Protector for PCs anfordern

In Data Protector for PCs ist ein Wartungsvertrag mit einjähriger Laufzeit enthalten. Dadurch haben Sie das Recht auf:

- Telefonische Unterstützung, direkter Kontakt zu einem Kundendiensttechniker.
- Aktualisierungen für den Data Protector for PCs-Server und die Data Protector for PCs-Agentensoftware. Sie können die neuesten Versionen oder ein CD-ROM-Image von der Data Protector-Website herunterladen. Rufen Sie dazu die Seite <http://www.hp.com/go/dataprotector> auf.

Glossar

Active Directory (*Windows-spezifischer Begriff*) Der Verzeichnisdienst in einem Windows-Netzwerk. Er enthält Informationen zu Ressourcen im Netzwerk und stellt sie Benutzern und Anwendungen zur Verfügung. Die Verzeichnisdienste sorgen dafür, dass Ressourcen einheitlich benannt, beschrieben, gesucht, aufgerufen und verwaltet werden, unabhängig vom physischen System, auf dem sie sich befinden.

Agent Data Protector for PCs-Software, die auf den Desktop-PCs/Notebooks der Benutzer ausgeführt wird. Sie kommuniziert via Webservices (SOAP und XML) über TCP-Port 80 mit dem Policy Server.

Anfangsaktualisierung

Data Protector for PCs schützt Dateien ununterbrochen, indem die von Benutzern vorgenommenen Änderungen gespeichert werden. Wenn ein Benutzer einen neuen Data Vault erstellt, muss Data Protector for PCs eine Anfangsaktualisierung für alle geschützten Dateien des Benutzers in den Vault durchführen. Benutzer können bestimmen, ob die Anfangsaktualisierung sofort oder im Hintergrund durchgeführt wird.

Benutzer mit Administratorrechten

Ein Benutzer auf dem Web-Data Vault-Server, der für administrative Aufgaben verantwortlich ist, wie das Erstellen und Löschen von Data Vaults und Mirrieren von Clientsicherungsdaten.

Benutzer mit Sicherungsrechten

Ein Benutzer auf dem Web-Data Vault-Server, der Endbenutzervorgänge wie das Sichern und Wiederherstellen von Dateien durchführt.

Benutzerkontrollrichtlinie

Diese Richtlinie bestimmt, wie viel Kontrolle die einzelnen Benutzer über die auf ihren Desktop-PCs/Notebooks/Laptops ausgeführte Agentensoftware haben. Sie können den Agenten sperren, sodass die Richtlinien vollständig vor den Benutzern verborgen sind, Sie können festlegen, dass die Benutzer die Richtlinien anzeigen, jedoch nicht ändern können, oder Sie können den Benutzern gestatten, eigene Richtlinien hinzuzufügen. Diese Berechtigungen können Sie für jede Data Protector for PCs-Hauptrichtlinie separat festlegen. Die Benutzerkontrollrichtlinie gilt für alle Benutzer.

Cleanup-Richtlinie

Die den Dateischutzrichtlinien zu Grunde liegenden Aufbewahrungsrichtlinien werden mithilfe von regelmäßig ausgeführten Cleanup-Aufgaben (Bereinigungsaufgaben) ausgeführt. Die Häufigkeit wird in der Cleanup-Richtlinie festgelegt. Standardmäßig werden die Local Repositories der Benutzer einmal pro Stunde bereinigt, und lokal definierte Data Vaults werden einmal pro Tag bereinigt. Bei zentral definierten Data Vaults in Windows-Dateifreigaben führt ein Computer, der über die Data Vault-Richtlinie zugewiesen wurde, das Cleanup durch. Bei Web-Data Vaults wird das Cleanup lokal auf dem Data Vault-Server ausgeführt. Die Cleanup-Richtlinie gilt für alle Benutzer.

Continuous File Protection

Continuous File Protection ist das Continuous Data Protection-Verfahren von Data Protector for PCs, durch das Änderungen an einer Datei bei jedem Speichervorgang automatisch gesichert werden. Dieses Verfahren eignet sich für vom Benutzer gespeicherte Datendateien (im Gegensatz zu Dateien, die immer geöffnet sind, wie z. B. Datenbanken oder Outlook-Dateien). Jede Continuous File Protection-Richtlinie schützt eine Gruppe von Dateien, die in irgendeiner Weise miteinander verbunden sind. In Data Protector for PCs sind bereits Richtlinien für die gängigsten Dateitypen vorkonfiguriert, z. B. Office-Dokumente und Bilder. Sie können diese Dateischutzrichtlinien an Ihre Anforderungen anpassen oder neue Richtlinien erstellen. Die Richtlinie gibt auch an, wie lang die Vorgängerversionen von geschützten Dateien aufbewahrt werden.

Data Vault

Es gibt zwei verschiedene Typen von Data Vaults:

- Web-Data Vaults. Diese verwenden das HTTPS-Protokoll und bieten höchste Sicherheit bei der Übertragung von Daten zwischen Client-PCs und dem Data Vault sowie einen höheren Durchsatz in Umgebungen mit hoher Latenz und werden daher empfohlen.
- Data Vaults in Windows-Dateifreigaben. Hierbei handelt es sich um freigegebene Ordner auf einem Dateiserver, in denen Dateien gemäß Data Vault-Richtlinie gespeichert werden. Der Dateiserver muss das Windows-Dateifreigabeprotokoll (CIFS/SMB) unterstützen. Diese Data Vaults sollten nicht in Umgebungen mit hoher Netzwerklatenz verwendet werden.

Die Datenstruktur beider Data Vault-Typen ist identisch, sodass Sie Data Vaults in Windows-Dateifreigaben in Web-Data Vaults konvertieren können.

Jedem Benutzer können auf der Grundlage seiner Mitgliedschaft in Gruppen oder Organisationseinheiten eine oder mehrere Data Vault-Richtlinien zugewiesen werden.

geschützte Dateien

Eine geschützte Datei ist eine Datei, die automatisch durch Data Protector for PCs gesichert wird. Die geschützten Dateitypen werden in den Continuous- und Open File Protection-Richtlinien definiert.

Konsole

Über die browserbasierte Konsole können Sie Data Protector for PCs-Richtlinien zentral definieren. Dafür müssen Sie Mitglied der Administratorengruppe sein.

Kopierrichtlinie

Kopierrichtlinien definieren Folgendes:

- Anzahl der Agenten, die gleichzeitig Dateien in Ihre Data Vaults kopieren können.
- Zeitplan für regelmäßige Aktualisierungen, bei denen geprüft wird, ob alle erwarteten Dateien für einen Benutzer auf dem Data Vault vorhanden sind. Falls dies nicht der Fall ist, werden die fehlenden Dateien kopiert. Damit wird noch einmal sichergestellt, dass alle Benutzerdateien ordnungsgemäß auf den Data Vault kopiert wurden.
- Ob eine *Anfangsaktualisierung* durchgeführt werden soll. Die Anfangsaktualisierung wird benötigt, da während des normalen Betriebs von Data Protector for PCs nur Informationen über die Änderungen in den Data Vault kopiert werden, wenn ein Benutzer eine von Data Protector for PCs im Continuous-Modus geschützte Datei ändert.

Nach der Installation von Data Protector for PCs muss eine Kopierrichtlinie definiert werden, um eine Anfangsaktualisierung aller geschützten Dateien Ihrer Benutzer durchzuführen.

Local Repository

Beim Local Repository handelt es sich um einen sicheren Speicherort auf Agentcomputern, an dem geschützte Dateien und Dateiänderungen gespeichert werden. Dieser Speicherort befindet sich meist auf der Systemfestplatte. Es handelt sich um ein verborgenes Systemverzeichnis. Die Benutzer können Vorgängerversion einfach und schnell durch einen Rechtsklick auf die Datei auf dem Desktop, im Windows Explorer oder über das Dialogfeld „Öffnen“ wiederherstellen. Dateien, die durch die Continuous File Protection-Richtlinien geschützt werden, werden so lange in einem verborgenen Verzeichnis auf dem lokalen Computer aufbewahrt, wie es der Aufbewahrungsrichtlinie entspricht. Dateien, die durch die Open File Protection-Richtlinien geschützt werden, werden vorübergehend im Local Repository gespeichert, bis sie in den Data Vault kopiert werden. Der Pfad zum Local Repository lautet in der Regel `C:\{DPNE}`.

Open File Protection

Die Open File Protection sichert Dateien, die immer geöffnet sind, z. B. persönliche Outlook-Ordner und zahlreiche Datenbankdateien, indem regelmäßig Momentaufnahmen auf Dateiebene angefertigt werden. Dies wird häufig als „annähernde“ Continuous Data Protection bezeichnet. In einer Open File Protection-Richtlinie wird mittels einer Reihe von Einschluss- und Ausschlussregeln der Schutz für offene Dateien definiert. Sie können z. B. eine Richtlinie mit dem Namen „Persönliche Outlook-Ordner“ definieren, die für .pst-Dateien von Outlook gilt, indem Sie die Einschlussregel „Endet mit ‚.pst‘“ definieren. Wenn Sie archivierte .pst-Dateien ausschließen möchten, können Sie

zusätzlich die Ausschlussregel „Enthält ,Archiv“ definieren. Richtlinien geben auch an, wie lang die Vorgängerversionen von geschützten Dateien aufbewahrt werden. Open File Protection-Richtlinien gelten für alle Benutzer.

Richtlinie

Eine Richtlinie ist ein zentral im Policy Server definierter Regelsatz, der von den einzelnen Agents auf den Desktop-PCs/Notebooks/Laptops der Benutzer ausgeführt wird.

Richtlinienserver

Der Policy Server verwaltet die Data Protector for PCs-Richtlinien zentral. Außerdem sammelt er Statusinformationen von den Agenten und liefert Berichte über deren Bereitstellung und Betrieb.

Stichwortverzeichnis

Symbole

.NET Framework, 15, 37

A

Active Directory

- Gruppen zu Data Vaults zuordnen, 28
- Zugriff, 28

Agent Deployment Kit, Inhalt, 39

Agent-Software

- unternehmensweit bereitstellen, 38

Agenten, 8

- Aktualisieren, 42
- Voraussetzungen, 13

Agentenaktualisierungsrichtlinie, 30

Agentenbereitstellung, Bericht, 43

Agentensoftware

- installieren, 37

Agents

- Anzahl der unterstützten, 32

Aktualisieren

- Agenten, 42
- Richtlinienserver, 42

Ändern

- Benutzer mit Administratorrechten, 21
- Benutzer mit Sicherungsrechten, 21

ASP.NET, 15

B

Befehlszeilenbefehle

- DPNECleanup, 35
- DvConfig, 21

Benutzer mit Administratorrechten

- Ändern, 21
- Erstellen, 19

Benutzer mit Sicherungsrechten

- Ändern, 21
- Erstellen, 19

Benutzercomputer, Voraussetzungen, 13

Benutzerkontrollrichtlinie, 30

Bereitstellen der Agent-Software, 38

- Fortschritt überprüfen, 40
- Prozedur, 39

Bereitstellung

- Fortschritt überprüfen, 40
- Prozedur, 39

Berichtsdatenerhalt, 30

Browsereinstellungen für Policy Server Console, 17

C

Cleanup-Richtlinie, 29

Cleanup-Software, 18

Continuous File Protection-Richtlinien, 27

D

Data Protector for PCs

- Agenten installieren, 37
- Architektur, 8
- Support anfordern, 45
- Übersicht, 8

Data Vault-Richtlinien, 24

Data Vaults

- Active-Directory-Gruppen zuordnen, 28
- Daten migrieren, 20
- Serverempfehlungen, 32
- Voraussetzungen, 25
- Web, 9
- Windows-Dateifreigabe, 9

Data Vaults in Windows-Dateifreigaben

- Migration von Daten aus, 20

Dateifreigabe, Data Vaults, 9

Dateischutzrichtlinien, 27

- Continuous, 27
- Open, 27

Dateiserver, 8

Daten in einen neuen Data Vault migrieren, 20

Datenbankvoraussetzungen, 13

Desktop-PCs, Voraussetzungen, 13

Dokument

- Konventionen, 5

Dokumentation

- Feedback einreichen, 7

DPNECleanup, 35

DvConfig, 21

E

EFS-verschlüsselte Dateien, 27

Eingabe eines Verschlüsselungspassworts, 31

Eingeben eines Lizenzschlüssels, 31

Erstellen

- Benutzer mit Administratorrechten, 19
- Benutzer mit Sicherungsrechten, 19

Exportieren eines Verschlüsselungspassworts, 23, 31

F

FQDN, 18

H

Hilfe

- Anfordern, 6

HP

- Technischer Support, 6

HTTPS-Protokoll, 9

I

IIS, 15

Importieren eines Verschlüsselungspassworts, 31

Importierte Zertifikate, 10

Installation mit Microsoft SharePoint, 17

installieren

Agenten, 37

Cleanup-Software, 18

Richtlinienserver, 14

SQL Server, 16

Übersicht, 11

Web-Data Vault-Server, 18

Internet Information Services, 15

K

Konfigurieren

Active-Directory-Zugriff., 28

Agentenaktualisierungsrichtlinie, 30

Benutzerkontrollrichtlinie, 30

Berichtsdatenerhalt, 30

Cleanup-Richtlinie, 29

Continuous File Protection-Richtlinien, 27

Data Vault-Richtlinien, 24

Dateischutzrichtlinien, 27

Erstkonfiguration von Richtlinien, 24

Kopierrichtlinien, 26

Multithread-Cleanup, 35

Open File Protection-Richtlinien, 27

Web-Data Vault-Server, 18

Konsole

Ausführen, 16

Browsereinstellungen, 17

Konsole ausführen, 24

Konventionen

Dokument, 5

Kopierrichtlinien, 26

L

Lizenzen

Verfügbare, 23

Verschieben, 31

Lizenzieren, 23, 30

Lizenzschlüssel

Eingeben, 31

M

Multithread-Cleanup, 35

N

Netzwerk, Sizing-Faktoren, 34

Notebooks, Voraussetzungen, 13

O

Open File Protection-Richtlinien, 27

P

Passwort, 23, 31

Policy Server Console

Ausführen, 16

Browsereinstellungen, 17

Policy Server Console ausführen, 24

R

Richtlinien

Agentenaktualisierung, 30

Benutzerkontrolle, 30

Berichtsdatenerhalt, 30

Cleanup, 29

Continuous File Protection, 27

Data Vault, 25

Dateischutz, 27

Erstkonfiguration, 24

Kopie, 26

Open File Protection, 27

Verteilung von, 8

Richtlinienserver, 8

Aktualisieren, 42

Datenbankvoraussetzungen, 13

Empfehlungen, 33

installieren, 14

Voraussetzungen, 12

S

Selbstsignierte Zertifikate, 10, 18

Server

Datei, 8

Richtlinie, 8

SharePoint

Installation des Policy Server, 17

Sizing-Faktoren, 32

Data Vault, 32

Netzwerk, 34

Richtlinienserver, 33

SQL Server

installieren, 16

SQL-Datenbank

Voraussetzungen, 13

SSL ändern, 21

SSL-Port

Ändern, 21

Eingeben, 18

Subscriber's Choice, HP, 6

T

Technischer Support, 6, 7

Testversion von Data Protector for PCs, 23, 31

U

- Übersicht, 8
- Unterstützung, 45
- Unterstützungsmatrix, 8

V

- Verschieben von Lizenzen, 31
- Verschlüsselungspasswort, 23, 31
- Vertrauenswürdige Zertifizierungsstelle, 11
- Voraussetzungen, 12

W

- Web-Data Vault-Server, 8
 - installieren, 18
 - Konfigurieren, 18
 - Voraussetzungen, 13
- Web-Data Vaults, 9
 - Löschen, 19
 - Migration von Daten in, 20
 - Verwalten, 19
- Web-Data Vaults löschen, 19
- Web-Data Vaults verwalten, 19
- Websites
 - HP, 7
 - HP Subscriber's Choice for Business, 6
- Windows Installer, 15, 37

Z

- Zertifikate, 10, 18
 - Austauschen, 11, 21
- Zertifikate austauschen, 11
- Zielgruppe, 5
- Zugriff auf Active Directory, 28