HP Data Protector Notebook Extension 6.21

Installations- und Administrationhandbuch

Teilenummer: n/v
Erste Ausgabe: Oktober 2010

Rechtlicher Hinweis und Informationen

Vertrauliche Computersoftware. Zum Besitz, zur Verwendung und zur Vervielfältigung ist eine gültige HP Lizenz erforderlich. Gemäß FAR 12.211 und 12.212 werden kommerzielle Computersoftware und das Begleitmaterial (Dokumentation und technische Daten) für US-Behörden unter der kommerziellen Standardlizenz des Anbieters lizenziert.

Die in diesem Dokument enthaltenen Informationen können jederzeit ohne Ankündigung geändert werden. Für HP Produkte und Services gilt ausschließlich die Herstellergarantie, die in den Garantieerklärungen der jeweiligen Produkte und Services explizit beschrieben wird. 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 XP®, Windows NT® und Windows Vista® sind eingetragene Warenzeichen der Microsoft Corporation.

Inhalt

Abbildungen

Tabellen

Informationen zu diesem Dokument

In diesem Handbuch sind Informationen zu Folgendem enthalten:

- HP Data Protector Notebook Extension installieren
- Richtlinien für HP Data Protector Notebook Extension konfigurieren
- Software "HP Data Protector Notebook Extension Agent" auf den Desktop-PCs und Notebooks der Benutzer
- Bestimmen, wieviele Agenten unterstützt werden können
- Unterstützung für Notebook Extension anfordern

Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die HP Data Protector Notebook Extension installieren und konfigurieren möchten. Vorkenntnisse in folgenden Bereichen sind von Vorteil:

- Windows-Administration

Dokumentkonventionen und -symbole

Tabelle 1 Dokumentkonventionen

Konventionen	Element
Blauer Text: Tabelle 1 auf Seite 7	Querverweislinks und E-Mail-Adressen
Blauer, unterstrichener Text: http://www.hp.com	Website-Adressen

Konventionen	Element
Gefetteter Text	• Tasten, die gedrückt werden • Text, der in ein Oberflächenelement, z. B. ein Feld, eingegeben wird • Oberflächenelemente, auf die geklickt wird oder die ausgewählt werden, z. B. Menü- und Listeneinträge, Schaltflächen und Kontrollkästchen
Kursiver Text	Betonter Text
`Nichtproportionaler Text`	• Datei- und Verzeichnisnamen • Systemausgabe • Code • Befehle, deren Argumente und Argumentwerte
`Nichtproportionaler, kursiver` Text	• Codevariablen • Befehlsvariablen
`Nichtproportionaler, gefetteter` Text	Betonter, nichtproportionaler Text

WICHTIG:

Enthält Erklärungen oder spezielle Anweisungen.

HINWEIS:

Enthält zusätzliche Informationen.

Allgemeine Informationen

Allgemeine Informationen zu Notebook Extension finden Sie unter http://www.hp.com/go/dataprotector.

Technischer Support von HP

Informationen zum technischen Support weltweit finden Sie auf der HP Support Website:

http://www.hp.com/support

Bevor Sie sich an HP wenden, stellen Sie folgende Informationen zusammen:

- Namen und Nummern des Produktmodells
- Registrierungsnummer für den technischen Support (falls zutreffend)
- Produktseriennummern
- Fehlermeldungen
- Betriebssystemtyp und Versionsnummer
- Detailfragen

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 folgenden HP Websites:

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

Feedback zur Dokumentation

HP freut sich über Ihr Feedback.

Wenn Sie Anmerkungen und Vorschläge zur Produktdokumentation machen möchten, senden Sie eine Nachricht an DP.DocFeedback@hp.com. Alle Einsendungen werden Eigentum von HP.

1 Übersicht und Voraussetzungen

Übersicht zu Notebook Extension

HP Data Protector Notebook Extension 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 Supportmatrix (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.

Mindestens ein Dateiserver muss vorhanden sein. Dateiserver enthalten gemeinsam genutzte Ordner, Data Vaults genannt, in die Notebook Extension bei der Sicherung die Benutzerdaten kopiert.

In der folgenden Abbildung ist die Notebook Extension-Architektur dargestellt:

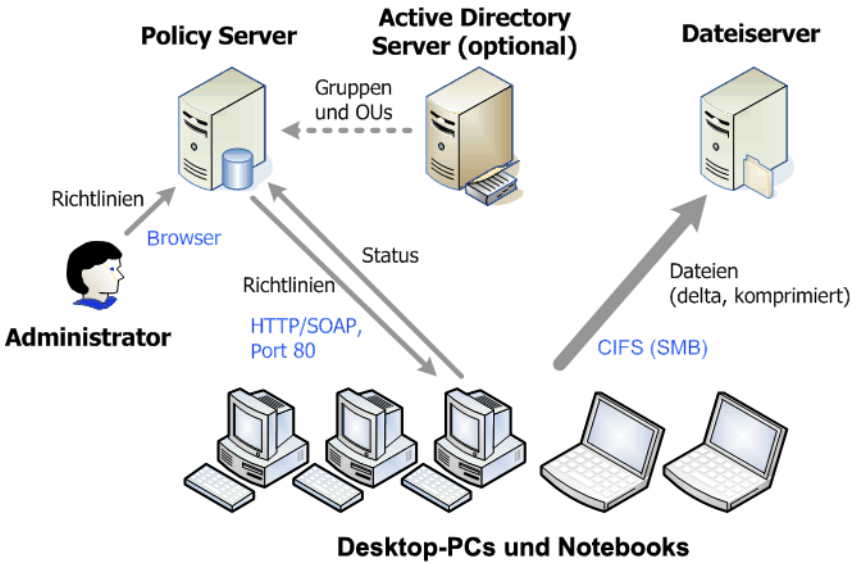

Abbildung 1 Notebook Extension-Architektur

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 Konsole definiert. Anschließend werden die Richtlinien automatisch mithilfe des SOAP-Protokolls über HTTP-Port 80 an die Agenten verteilt. Die Richtlinien befinden sich auf dem Policy Server.

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-Konsole generiert werden.

Data Vaults befinden sich auf Dateiservern. Für eine bessere Leistung empfiehlt es sich, auf diesen Servern außer der Cleanup-Software keine andere Notebook Extension-Software auszuführen.

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.

Übersicht zur Installation von Notebook Extension

Die Installation von Notebook Extension umfasst drei Schritte:

1. **Installieren Sie den Notebook Extension Policy Server.**

   Informationen hierzu finden Sie Kapitel 2 auf Seite 17

2. **Konfigurieren Sie Schutzrichtlinien.**

   Informationen hierzu finden Sie Kapitel 3 auf Seite 23

3. **Installieren Sie Notebook Extension-Agenten auf Laptop- und Desktopcomputern.**

   Informationen hierzu finden Sie in Kapitel 4 auf Seite 37

Voraussetzungen

Policy Server

Informationen zu unterstützten Betriebssystemen finden Sie in der Supportmatrix.

HINWEIS:

Installation auf einem Windows 2003-Betriebssystem (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 während der Installation beim Überprüfen der Voraussetzungen erkannt. Sie haben dann die Möglichkeit, den 32-Bit-Modus für IIS festzulegen. Wenn auf dem Server andere Webanwendungen vorhanden sind, für die IIS im 64-Bit-Modus ausgeführt werden muss (z. B. Microsoft Exchange 2007 mit Web-Mail - Outlook Web Access), können Sie den Policy Server nicht auf diesem Server installieren. Dies gilt nicht für die Installation eines Policy Servers 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

  Unter Windows 2003 wird IIS 6.0 vorausgesetzt und muss vor dem Policy Server installiert werden. Unter Windows 2008 bietet Notebook Extension die Installation von IIS 7.0 und 7.5 an, sofern nicht bereits installiert.

- 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)

Ebenfalls nur für Internet Information Services 7.0 und 7.5 werden die folgenden IIS-Komponenten benötigt. Wenn sie nicht installiert sind, wird Ihnen vom Assistenten die Option angeboten, sie zu installieren.

- IIS Static Content Web Server - erforderlich für die Bereitstellung von statischen HTML-Dateien, von Dokumenten und von Bildern
- IIS ASP.NET - erforderlich für die Bereitstellung von ASP.NET 2.0 und des .NET Framework
- IIS Security - erforderlich für die Verwendung der integrierten Windows-Authentifizierung für die Policy Server-Konsole.
- IIS 6 Management Compatibility - ermöglicht es, IIS 6 und IIS 7 möglichst einheitlich zu konfigurieren

Datenbank

Notebook Extension benötigt den Zugriff auf eine Microsoft SQL Server-Datenbank. Informationen zu unterstützten Versionen finden Sie in der Supportmatrix.

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**). Wenn dies nicht der Fall ist, aktivieren Sie die Option, und klicken Sie auf **OK**.

Sie können auch während der Installation von Notebook Extension eine Instanz von Microsoft SQL Server Express Edition installieren.

Notebook Extension-Agenten

Die Notebook Extension-Agentensoftware kann auf Benutzerdesktops und -notebooks installiert werden, auf denen Windows installiert ist. Informationen zu unterstützten Plattformen finden Sie in der Supportmatrix.

2 Notebook Extension Policy Server installieren

HINWEIS:

Um eine vorhandene Installation des Notebook Extension Policy Servers auf eine neuere Version zu aktualisieren, befolgen Sie die Standardinstallationsprozedur. Weitere Informationen hierzu finden Sie im Abschnitt “Policy Server aktualisieren” auf Seite 21.

Schnellinstallation

Im Abschnitt Policy Server auf Seite 13 finden Sie Informationen zu den Voraussetzungen für den Notebook Extension Policy Server.

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Befolgen Sie die angezeigten Anweisungen.
3. Der Notebook Extension Policy Server benötigt den Zugriff auf eine Microsoft SQL Server-Datenbank. Wählen Sie **Vorhandene DataProtectorNE-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 Seite **Data Protector Notebook Extension Policy Server installieren** des Assistenten auf **Installieren**, um die Installation zu starten.

5. Wenn die Installation abgeschlossen ist, müssen Sie die Cleanup-Software installieren. Klicken Sie in der Anzeige **Data Protector Notebook Extension Data Vault Cleanup installieren** auf **Installieren**.
6. Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**. Anschließend können Sie die Notebook Extension Policy Server-Konsole starten.

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.

Benutzerdefinierte Installation

HINWEIS:

Nur Windows 2003-Server: Der Notebook Extension Policy Server kann nur dann von einer im Netzwerk freigegebenen CD-ROM oder von einer Netzwerkdateifreigabe installiert werden, wenn die Laufzeitsicherheitsrichtlinie für NET 2.0 Framework bei diesem Server für die Sicherheitszone "Lokales Intranet" auf *Voll vertrauenswürdig* eingestellt 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 Notebook Extension Policy Servers durchführen zu können, müssen Sie bei einem Konto mit Administratorrechten angemeldet sein.

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der 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 **Speichern** aus.

3. Der Notebook Extension 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 diese Anwendung nicht installiert ist, werden Sie gefragt, ob Sie Windows Installer 3.1 von der CD installieren möchten.

4. Der Installationsassistent prüft, ob die folgende erforderliche Software installiert ist:

   - Internet Information Services (IIS)
   - ASP.NET 2.0

   Wenn eine dieser Komponenten nicht vorhanden ist, 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.

   So verwenden Sie eine vorhandene Instanz von Microsoft SQL Server:

   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 die Felder **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 ein Test der Verbindung zum vorhandenen Datenbankserver durchgeführt. Wenn der Test erfolgreich ist, geht der Assistent zu Schritt 6 über.

   So installieren Sie die Notebook Extension-Instanz der 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 dem Namen "DataProtectorNE" zu installieren. Klicken Sie auf **Weiter**, wenn die Installation abgeschlossen ist.

6. Installieren Sie den Notebook Extension Policy Server.

   a. Klicken Sie auf der Eingangsanzeige auf **Weiter**, um die Installation zu starten.
      - Die Notebook Extension Policy Server-Konsole wird als Webanwendung im virtuellen Verzeichnis `C:\Inetpub\wwwroot\dpnepolicy` installiert.

- Der Webservice von Notebook Extension 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 Servers 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**.

Notebook Extension wird zentral über die Notebook Extension Policy Server-Konsole verwaltet. Da die Konsolebrowserbasiert ist, können Sie Notebook Extension von jedem Computer aus verwalten,der eine Browserverbindung zum Policy Server herstellen kann (über HTTP-Port 80).

Um die Notebook Extension mit einem Browser auf dem Policy Server auszuführen, lassen Sie die Option **Policy Server-Konsole ausführen** markiert, und klicken Sie auf **Fertig stellen**.

HINWEIS:

Während der Installation wird auf dem Policy Server die Cleanup-Software installiert. Zur Optimierung der Leistung empfiehlt es sich außerdem, die Software in den Data Vaults zu installieren.

HINWEIS:

Browsereinstellungen für die Policy Server-Konsole: Wenn Sie Probleme beim Anzeigen der Policy Server-Konsole in Ihrem Browser haben, überprüfen Sie die Browsersicherheitseinstellungen. Für die Konsole ist folgendes erforderlich:

- JavaScript muss aktiviert sein.
- Für die dpnepolicy-Website müssen Popups aktiviert sein.
- Je nach Art und Version des verwendeten Browsers müssen möglicherweise noch weitere Sicherheitseinschränkungen geändert werden.

Installation mit Microsoft SharePoint: Wenn der Policy Server auf einem Server installiert wird, auf dem Microsoft SharePoint ausgeführt wird, wird möglicherweise die Fehlernachricht "404 - Die Seite kann nicht angezeigt werden" angezeigt, wenn Sie die Policy Server-Konsole ausführen. Der Fehler und die Maßnahmen zur Fehlerbehebung werden im folgenden Microsoft Knowlege Base-Artikel beschrieben: http://support.microsoft.com/kb/828810. Dieser Fehler tritt bei allen ASP.NET-Webanwendungen auf, nicht nur beim Policy Server.

Wenn Sie den Policy Server auf einem Server mit SharePoint ausführen möchten, müssen Sie wie folgt vorgehen:

1. Erstellen Sie mithilfe der SharePoint-Administrationswerkzeuge Ausschlussregeln für die beiden Policy Server-Webanwendungen: `dpnepolicy` und `dpnepolicyservice`.
2. Fügen Sie den beiden `web.config`-Dateien des Policy Servers (`dpnepolicy\web.config` und `dpnepolicyservice\web.config`) den XML-Code `<httpHandlers>` und `<trust>` hinzu, wie im zuvor erwähnten Microsoft Knowledge Base-Artikel beschrieben.

Policy Server aktualisieren

Um eine vorhandene Installation des Notebook Extension Policy Servers auf eine neuere Version zu aktualisieren, befolgen Sie die Standardinstallationsprozedur. Alle vorhandenen Konfigurationen (z. B. Data Vault-Konfiguration, Lizenzierung usw.) stehen in der neueren Version zur Verfügung.

Vorhandene Agenten, die die Vorversion von Notebook Extension verwenden, funktionieren weiterhin wie bisher. Sie können sie manuell oder mithilfe der Agentenaktualisierungsrichtlinie im Hintergrund aktualisieren. Weitere Informationen hierzu finden Sie im Abschnitt “Agenten aktualisieren” auf Seite 42.

Aktualisierungsprozedur:

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf der Seite "Data Protector Notebook Extension installieren" des Assistenten auf **Policy Server installieren**, um das Upgrade zu starten.
3. Befolgen Sie die angezeigten Anweisungen.
4. Bei der Installation wird die vorhandene Policy Server-Installation erkannt und die Aktualisierung angeboten.
5. Befolgen Sie die angezeigten Anweisungen.
6. Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**. Anschließend können Sie die Notebook Extension Policy Server-Konsole starten.

HINWEIS:

Wenn auf dem Policy Server die Cleanup-Software installiert ist, müssen Sie sie auch aktualisieren. Sie können sie manuell oder mithilfe der Agentenaktualisierungsrichtlinie aktualisieren.

3 Notebook Extension-Schutzrichtlinien konfigurieren

Ersteinrichtung nach der Installation von Notebook Extension

Direkt nach der Installation von Notebook Extension wird in der Policy Server-Konsole das Fenster für die Ersteinrichtung angezeigt. Um Richtlinien für Notebook Extension einrichten zu können, müssen Sie zunächst zwei Konfigurationsschritte erfolgreich durchführen:

1. **Definieren oder importieren Sie ein Verschlüsselungspasswort.**

   Aus Sicherheitsgründen müssen Sie ein Verschlüsselungspasswort definieren, bevor Sie Notebook Extension 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-Konsole) definierte Data Vaults verwenden zur Verschlüsselung immer das Notebook Extension-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 Notebook Extension 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 Notebook Extension.**

   Mit der Testversion von Notebook Extension können Sie 60 Tage lang ohne Lizenz eine unbegrenzte Anzahl von Benutzern schützen. Wenn Sie Notebook Extension kaufen, müssen Sie den HP License Key Delivery Service unter https://webware.hp.com/welcome.asp besuchen, um einen Lizenzschlüssel herunterzuladen, den Sie dann eingeben können. 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. Wenn Sie dies nicht tun, können die Agenten nach 60 Tagen keine Daten mehr in ihre Local Repositories oder Data Vaults kopieren. Allerdings können zuvor geschützte Dateiversionen immer noch wiederhergestellt werden.

   Klicken Sie zur Verwaltung der Lizenzen auf **Lizenzverwaltung** und auf **Geben Sie einen Lizenzschlüssel für Benutzer von Data Protector Notebook Extension ein**. Befolgen Sie die angezeigten Anweisungen.

HINWEIS:

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

Nach Abschluss dieser Konfigurationsschritte steht Ihnen der volle Funktionsumfang der Policy Server-Konsole zur Verfügung. Wenn Sie Notebook Extension soeben erst installiert haben, konfigurieren Sie die weiteren Elemente von Notebook Extension in der im nächsten Abschnitt angegebenen Reihenfolge.

Erstkonfiguration

In Notebook Extension sind verschiedene Richtlinien vorkonfiguriert, die für die meisten Organisationen ausreichen. Es wird empfohlen, zuerst Data Vault-, Kopie-

und Dateischutzrichtlinien zu konfigurieren und anschließend die Notebook Extension-Agentensoftware auf den Desktop-PCs und Notebooks der Benutzer zu installieren.

HINWEIS:

Statt neue Richtlinien zu konfigurieren, können Sie auch die vorkonfigurierten Richtlinien von Notebook Extension ändern. Klicken Sie einfach auf **Vorhandene Richtlinie bearbeiten**, statt in den einzelnen Schritten jedes Mal **Neue Richtlinie erstellen** auszuwählen.

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

1. Sie können die Notebook Extension Policy Server-Konsole nach Abschluss des Installationsassistenten ausführen oder zu jedem beliebigen anderen Zeitpunkt über die folgende URL aufrufen:

   `http://policyserver/dpnepolicy/`

   Dabei steht "*policyserver*" für den Namen Ihres Notebook Extension Policy Servers. Sie müssen als Administrator beim Server angemeldet sein.

2. **Data Vault-Richtlinien konfigurieren**.

   In Data Vault-Richtlinien wird das Speicherziel für die kontinuierliche Sicherung von durch Richtlinien geschützten Benutzerdateien angegeben. Wenn eine Datei geändert wird, können die Vorgängerversion und die geänderte Datei automatisch an einem oder mehreren Speicherzielen gesichert werden. Ein Zielort ist meistens eine Netzwerkfreigabe. 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* zuordnen.

   Voraussetzungen für Data Vaults:

   Notebook Extension verwendet zum Speichern der geschützten Dateien, die von den Desktop-PCs und Notebooks der Benutzer gesichert werden, normale Windows-Dateifreigaben. Die Dateifreigaben sollten sich auf einem Windows Dateiserver befinden, der sich nicht auf demselben Computer wie der Policy Server befinden muss. Wenn Sie jedoch nur die Testversion von Notebook Extension mit einer kleineren Anzahl von installierten Agenten verwenden, ist es möglicherweise praktischer, für den Policy Server und den Data Vault-Dateiserver denselben Computer zu verwenden.

Notebook Extension legt für die auf dem Dateiserver gesicherten Dateien die gleichen Zugriffsberechtigungen (ACLs) fest, die für die Originaldatei gelten. Dies bedeutet, dass die Benutzer gesicherte Dateien nur wiederherstellen können, wenn Sie die ursprünglichen Dateien auf ihren Computern öffnen können.

So erstellen Sie eine Data Vault-Richtlinie:

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

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 „Kopierichtlinie“ zunächst unverändert bei „Standard“.

Für das Cleanup:

- 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. **Kopierichtlinien konfigurieren**.

Eine Kopierichtlinie begrenzt die Anzahl der Benutzercomputer, die gleichzeitig in einen Data Vault kopieren können. Außerdem definiert sie Anfangsaktualisierungen und geplante Aktualisierungen des Data Vaults zur Ergänzung der kontinuierlichen Sicherung. 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.
- 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** (oder -kopie) durchgeführt werden soll. Die Anfangsaktualisierung wird benötigt, da während des normalen Betriebs von Notebook Extension nur Informationen über die Änderungen in den Data Vault kopiert werden, wenn ein Benutzer eine von Notebook Extension 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.

So erstellen Sie eine Kopierichtlinie:

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 Dateikopien 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 lange 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.

  Notebook Extension enthält mehrere Beispielrichtlinien. Nach der Installation sind drei standardmäßig ausgewählt: *Office-Dokumente*, *Software-Entwicklung* und *Webdokumente*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

- **Open File Protection** – schützt die Dateien, indem in regelmäßigen Abständen (in der Regel 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 die Menüoption **Speichern** verfügt, mit diesem Verfahren geschützt werden. Häufig vorkommende Dateien diesen Typs sind E-Mail- und Datenbankdateien.

  In Notebook Extension sind dazu vier Beispiele vorhanden: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* und *Mozilla Thunderbird*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

HINWEIS:

Notebook Extension unterstützt nicht die Sicherung von mit EFS (Encrypting File System) verschlüsselten Dateien mit Open File Protection-Richtlinien. Daher dürfen Dateien wie beispielsweise .pst-Dateien nicht mit EFS verschlüsselt sein.

So erstellen Sie eine Dateischutzrichtlinie:

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 Dateien ohne Erweiterungen auswählen. Bei Continuous File Protection-Richtlinien ist dies nicht möglich.

WICHTIG:

Sie haben nun alle grundlegenden Richtlinien konfiguriert, die Notebook Extension benötigt. In Notebook Extension 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 Kapitel 4 auf Seite 37). Später können Sie die restlichen Notebook Extension-Richtlinien prüfen und konfigurieren, z. B. die Cleanup-Richtlinie, die Benutzerkontrollrichtlinie, die Agentenaktualisierungsrichtlinie und die Richtlinie für den Erhalt von Berichtsdaten.

Weitere Richtlinien konfigurieren

1. **Konfigurieren Sie den Active Directory-Zugriff**.

HINWEIS:

Active Directory-Gruppen mit Data Vaults verknüpfen: Sie können in der Data Vault-Richtlinie Data Vaults mit Active Directory-Gruppen verknüpfen. Alle Mitglieder der verknüpften Gruppen erstellen ihre Sicherungen im verknüpften Data Vault. Sie können keine einzelnen Benutzer verknüpfen. Wenn Sie eine Organisationseinheit verknüpfen, werden nur die Gruppen innerhalb dieser Organisationseinheit verknüpft. Benutzer direkt innerhalb der Organisationseinheit, werden nicht mit dem Data Vault verknüpft. Möglicherweise enthält die Liste der Active Directory-Gruppen fälschlicherweise außer Sicherheitsgruppen noch weitere Gruppen, wie z. B. Verteilungsgruppen. Es werden jedoch nur Sicherheitsgruppen mit dem Data Vault verknüpft.

Mehrere Benutzer: Wenn ein Computer von mehreren Benutzern verwendet wird, müssen diese Benutzer zur selben 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” auf Seite 24).

So konfigurieren Sie den Active-Directory-Zugriff:

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 auf den Benutzercomputern und die Data Vaults auf den Dateiservern muss regelmäßig ein Cleanup durchgeführt werden, um Versionen zu entfernen, die gemäß den Erhalteinstellungen in den Dateischutzrichtlinien zu alt sind.

So konfigurieren Sie die Cleanup-Richtlinie:

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-Administationskonsole 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 h.
- Für Samstag wählen Sie eine Startzeit am frühen Abend, wie z. B. 1 h.

Die Ausführung des Cleanups nur am Wochendene hat folgende Auswirkungen:

- Die Liste der Dateien, die zur Wiederherstellung von einem Data Vault angeboten werden, ist bis zu eine Woche alt. Benutzer können manuell eine erneute Durchsuchung ihrer Daten im Data Vault auslösen, um eine aktuelle Ansicht zu erhalten.
- Sicherungsversionen bleiben noch bis zu eine Woche nach ihrer Veralterung erhalten, weil der Cleanup nur an Wochenenden ausgeführt wird.
- Die Kontingentverwaltung ist nicht aktuell. Wenn Benutzer ihr Kontingent überschreiten, müssen sie möglicherweise bis zur Ausführung des Cleanups warten, bis sie wieder freien Speicherplatz im Data Vault erhalten. Andererseits wird möglicherweise eine Kontingentüberschreitung vom System nicht sofort erkannt, weil die Berechnung der Speicherbelegung Teil des Cleanup-Prozesses ist.

Empfohlene Einstellungen:

- **Cleanup-Zeitplan für Local Repository**: Behalten Sie den Standardwert von 1 Stunde bei.

- **Cleanup-Zeitplan für Data Vault**: Die Standardeinstellung (Cleanup täglich um Mitternacht) sollte für die meisten Installationen geeignet sein. Weitere Informationen zur Kapazität von Data Vaults finden Sie unter "Sizing-Empfehlungen" auf Seite 34.

3. **Konfigurieren Sie die Benutzerkontrollrichtlinie**.

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

   So konfigurieren Sie die Benutzerkontrollrichtlinie:

   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 **Selbständige Wiederherstellung** die Einstellung **Benutzerkontrolle zulassen** aus.

4. **Konfigurieren Sie die Richtlinie für die Agentenaktualisierung**.

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

   So konfigurieren Sie die Agentenaktualisierungsrichtlinie:

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

5. **Erhalt von Berichtsdaten konfigurieren**.

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

   So konfigurieren Sie den Erhalt von Berichtsdaten:

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

Weitere Konfigurationsschritte

Diese Schritte werden normalerweise bei der Erstinstallation von Notebook Extension durchgeführt.

Lizenzieren Sie Ihre Notebook Extension-Software.

Mit der Testversion von Notebook Extension können Sie 60 Tage lang ohne Lizenz eine unbegrenzte Anzahl von Benutzern schützen. Wenn Sie Notebook Extension kaufen, müssen Sie den HP License Key Delivery Service unter https://webware.hp.com/welcome.asp besuchen, um einen Lizenzschlüssel herunterzuladen, den Sie dann eingeben können.

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 Data Protector Notebook Extension 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 eine IP-Adresse des Policy Servers 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 Notebook Extension 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-Konsole) definierte Data Vaults verwenden zur Verschlüsselung immer das Notebook Extension-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 Notebook Extension 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 sicheren Speicherort abgelegt. Später können Sie es zum Importieren verwenden.

HINWEIS:

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

So verwalten Sie ein Verschlüsselungspasswort:

1. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
2. Klicken Sie auf **Verschlüsselungsrichtlinie**.
3. Befolgen Sie die angezeigten Anweisungen.

Bestimmen, wieviele Agenten unterstützt werden können

Es ist nicht ganz einfach, generelle Regeln festzulegen, die für alle Umgebungen zutreffen. Daher wird in den hier erläuterten Fällen klar der Kontext beschrieben, für den die angegebenen Zahlen zutreffen.

Sizing-Faktoren

Das Sizing für eine Notebook Extension-Umgebung ist komplex. Es gibt u.a. folgende technische Faktoren, die die Anzahl der Benutzer beeinflussen, die in einer bestimmten Umgebung unterstützt werden können:

- Die Verarbeitungsleistung in einem Data Vault (bei der Konsolidierung der Sicherungsdaten in der Nacht)
- Netzwerk- und E/A-Bandbreite auf dem Data Vault-Server
- Plattenspeicherplatz auf dem Data Vault-Server
- Größe der SQL Server-Datenbank auf dem Policy Server
- Netzwerkbandbreite und Verarbeitungsleistung auf dem Policy Server

Welcher dieser Faktoren einen Engpass in einer bestimmten Installation darstellen kann, wird durch die Konfigurationseinstellungen und Nutzungsmuster in Notebook Extension bestimmt:

- Anzahl der Benutzer in einem Data Vault
- Anzahl und Größe der von den Dateischutzrichtlinien abgedeckten Richtlinien

- Änderungshäufigkeit der geschützten Dateien
- Erhalteinstellungen für geschützte Dateitypen

Sizing-Empfehlungen

Data Vault

Folgende Hardwarespezifikationen bilden eine solide Basis für einen Data Vault:

- 1 x 3 GHz Dual-Core-Prozessor
- 2 GB RAM
- 7,5 TB Festplattenspeicherkapazität

Bei täglichem Cleanup kann ein solcher Data Vault eine Benutzerpopulation von bis zu **1.700** Agenten unterstützen, wenn sich das durchschnittliche Datenaufkommen wie folgt charakterisieren lässt:

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

Wenn Sie durchschnittlich mehr Daten schützen müssen, als in diesem Beispiel angegeben, schafft eine einfache Erhöhung der Festplattenkapazität auf dem Data Vault zwar mehr Platz für Daten, aber der Data Vault kann die Konsolidierung der Sicherungsdaten in der Nacht nicht mehr auf effiziente Weise durchführen. Folgende Möglichkeiten bieten in diesem Fall Abhilfe:

- Führen Sie den Cleanup für den Data Vault nur am Wochenende durch. Ausführliche Anweisungen hierzu finden Sie in Schritt 2 “Konfigurieren Sie die Cleanup-Richtlinie” im Abschnitt “Weitere Richtlinien konfigurieren” auf Seite 29. Wenn man von demselben durchschittlichen Datenaufkommen und einer Gesamtgröße des Data Vaults von 20 TB ausgeht, sollten Sie hierdurch die Anzahl der Agenten, die von einem Data Vault unterstützt werden können, auf 5000 erhöhen können.
- Verteilen Sie Endbenutzerdaten auf mehrere Data Vaults.

Wenn Ihre Benutzer im Durchschnitt weniger Daten haben, können Sie eventuell eine höhere Anzahl von Benutzern auf einem Data Vault hosten.

HINWEIS:

Um die bestmögliche Leistung zu erzielen, empfiehlt HP, das Betriebssystem auf dem Data Vault und die Sicherungsdaten auf physisch getrennten Festplatten zu speichern.

Für eine optimale Leistung sollte die Data Vault-Festplatte regelmäßig defragmentiert werden.

Policy Server

Die Menge des Datenverkehrs, der auf dem Policy Server generiert wird, hängt direkt von der Anzahl der Agenten ab, die von einem Server gehostet werden. Die in DPNE enthaltene Express Edition von MS SQL Server legt eine maximale Datenbankgröße von 4 GB fest, wobei nicht mehr als 5.000 Agenten[1] unterstützt werden können.

Wenn Sie mehr als 5.000 Agenten in Ihrer Umgebung unterstützen müssen, können Sie entweder zusätzliche Policy Server einsetzen oder MS SQL Express durch eine Vollversion von Microsoft SQL Server ersetzen. So kann der Policy Server ohne weiteres bis zu 50.000 Agenten unterstützen. Wenn Sie die Vollversion von MS SQL Server verwenden möchten, sollten Sie den Hauptspeicher des Policy Servers auf mindestens 3 GB aufrüsten.

Ein Policy Server kann auf demselben Server wie der Data Vault oder getrennt ausgeführt werden.

Es wird mindestens ein Policy Server benötigt, aber nicht unbedingt eine identische Anzahl von Data Vaults und Policy Servern.

Überlegungen bei Netzwerken

Normalerweise empfiehlt HP die Durchführung einer Anfangsaktualisierung von Notebook Extension Agenten auf Data Vaults nicht, wenn die Latenz (Verzögerungszeit) des Netzwerks zwischen den beiden höher als 50 ms ist. Dies gilt in der Regel für Home oder Remote Offices mit einer langsamen WAN-Verbindung. Die Anfangsaktualisierung funktioniert zwar, dauert aber sehr lange.

Wenn Ihre Umgebung Büros an mehreren Standorten umfasst und die Netzwerklatenz für einige von diesen größer als 50 ms ist, sollten Sie Data Vaults an mehr als einem Ort installieren, damit alle Büros mindestens einen Data Vault mit einer Latenz von 50 ms oder weniger erreichen können.

[1] Unter Verwendung der Standardeinstellung für den "Erhalt von Berichtsdaten" auf dem Policy Server von 30 Tagen.

Sobald die Anfangsaktualisierung beendet ist, können von jedem Standort in Ihrem Unternehmensnetzwerk oder sogar von einem Home Office aus Aktualisierungen durchgeführt werden. Diese sind in der Regel klein genug, damit sie auch über langsame Netzwerkverbindungen gut funktionieren.

Wenn die Anfangsaktualisierung über eine Hochlatenzverbindung durchgeführt werden muss, kann dies mehrere Tage in Anspruch nehmen. Sie kann jedoch ohne Probleme unterbrochen werden. Die Aktualisierung wird von Notebook Extension an dem Punkt wieder aufgenommen, an dem sie unterbrochen wurde, sobald die Verbindung zum Data Vault wiederhergestellt wird.

TIPP:

Wenn Sie nicht wissen, wie hoch die Latenz zwischen Ihren Büros ist, verwenden Sie den `ping`-Befehl von einem Computer an einem Standort, um die Erreichbarkeit eines Computers an einem anderen Standorts sowie die Dauer des Datenverkehrs zwischen den beiden festzustellen. Bei jedem erfolgreichen ping-Befehl wird die Latenz angegeben.

4 Notebook Extension-Agenten installieren

HINWEIS:

Wenn Sie den Notebook Extension-Server aktualisieren, aktualisieren Sie *alle* Agenten, bevor Sie Schutzrichtlinein für Dateien ohne Erweiterungen erstellen oder aktivieren. Sie können sie manuell oder mithilfe der Agentenaktualisierungsrichtlinie im Hintergrund aktualisieren. Weitere Informationen hierzu finden Sie im Abschnitt "Agenten aktualisieren" auf Seite 42.

OFP-Richtlinien, die Dateien ohne Erweiterung enthalten, können von DPNE-Agenten vor Version 6.21 nicht verarbeitet werden und werden ignoriert. Sofern nicht sämtliche Agenten aktualisiert wurden, können neuere Agenten Sicherungsdaten für Dateien ohne Erweiterung generieren, während auf einigen Data Vaults noch Cleanup-Agenten der alten Version eingesetzt werden. Beim Cleanup werden diese Sicherungen gelöscht, weil diese neuen Richtlinien nicht erkannt werden. Die entsprechenden Daten gehen verloren.

Aufgrund dessen ist die mit diesem Release eingeführte Thunderbird-Richtlinie standardmäßig deaktiviert.

HINWEIS:

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

Es gibt zwei Möglichkeiten, Notebook Extension-Agenten zu installieren:

- Installation auf allen Benutzercomputern einzeln. Informationen hierzu finden Sie in "Notebook Extension-Agenten auf einzelnen Benutzercomputern installieren" auf Seite 38

- Unternehmensweite Bereitstellung über einen Dateiserver, auf den alle Benutzercomputer zugreifen können. Informationen hierzu finden Sie in "Notebook Extension-Agenten unternehmensweit bereitstellen" auf Seite 39

Notebook Extension-Agenten auf einzelnen Benutzercomputern installieren

Voraussetzungen

Die Notebook Extension-Agentensoftware kann auf Benutzerdesktops und -notebooks installiert werden, auf denen Windows installiert ist. Informationen zu unterstützten Plattformen finden Sie in der Supportmatrix.

Sie müssen mit einem Konto mit Administratorrechten angemeldet sein.

Installationsprozedur

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Der Installationsassistent sollte automatisch gestartet werden. Andernfalls starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf **Data Protector Notebook Extension 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 die 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 die 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 Notebook Extension-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**. Sie werden aufgefordert, Ihr System erneut zu starten, falls auf dem Policy Server eine Open File Protection-Richtlinie definiert ist.

Jetzt sollte das Notebook Extension-Symbol im Infobereich angezeigt werden (je nach Schutzstatus eines dieser Symbole: ).

7. Prüfen Sie, ob der Notebook Extension-Agent ordnungsgemäß ausgeführt wird:
   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 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 Notebook Extension-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 Zeitmarke versehen, angezeigt werden. Wenn Sie eine der Versionen auswählen, wird das Dokument in der entsprechenden Anwendung im Nur-Lese-Modus geöffnet. Auf diese Weise können Benutzer ältere Versionen ihrer Dokumente aus dem lokalen Notebook Extension-Repository wiederherstellen.
8. Wiederholen Sie die Schritte 1 bis 8 für alle anderen Desktop-PCs und Notebooks, die mit Notebook Extension geschützt werden sollen.

Notebook Extension-Agenten unternehmensweit bereitstellen

Für die Erstinstallation können Sie Notebook Extension-Agenten mithilfe des Notebook Extension Agent Deployment Kits, das auf der Installations-CD-ROM enthalten ist, unternehmensweit bereitstellen

HINWEIS:

Sie können das Deployment Kit auf Vista-PCs, auf denen die Benutzerkontensteuerung aktiviert ist, nicht verwenden. Um dieses Problem zu beheben, deaktivieren Sie die Benutzerkontensteuerung, oder installieren Sie den Agenten interaktiv.

In der im Folgenden beschriebenen Prozedur kopieren Sie das Notebook Extension Agent Deployment Kit aus dem Ordner `CD-ROM:\Agent` in ein Verzeichnis auf einem Dateiserver, auf das alle Benutzer zugreifen können. Anschließend erstellen Sie in diesem Verzeichnis mithilfe von `SetupConfig.exe` eine Parameterdatei.

Zum Schluss richten Sie einen Mechanismus ein, mit dem die Datei `StartInstall.exe` im gemeinsam genutzten Verzeichnis von jedem Benutzercomputer aus ausgeführt werden kann. Hierfür können Sie z. B. ein Anmeldescript verwenden. Anschließend können Sie die Bereitstellung über die Notebook Extension Policy Server-Konsole von Agent mithilfe des Agentenbereitstellungsberichts überwachen.

Inhalt des Kits

Das Notebook Extension Deployment Kit enthält die folgenden Komponenten:

`SetupConfig.exe`	Erstellt und bearbeitet die Initialisierungsdatei.
`StartInstall.exe`	Startet die Datei `Setup.exe` als privilegierter Benutzer.
`Setup.exe`	Installiert die Voraussetzungen und die Datei `DataProtectorNE.ini`.
`DataProtectorNE.msi`	Windows Installer-Paket für Notebook Extension zur Installation der Agentensoftware.
`DataProtectorNE64.msi`	Windows Installer-Paket für Notebook Extension zur Installation der Agentensoftware auf 64-Bit-Systemen.
`DataProtectorNE*.*.mst`	Windows Installer-Pakete für Notebook Extension 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 Installation von Notebook Extension. Diese Datei wird von der Datei `SetupConfig.exe` (siehe Schritt 4 unten) erstellt.

Bereitstellungs- und Installationsprozedur

1. Kopieren Sie die Dateien aus dem Verzeichnis „Agent“ der Verteilungs-CD-ROM in ein Verzeichnis, auf das alle Benutzer, die das Notebook Extension Deployment Kit verwenden werden, zugreifen können. Dabei kann es sich beispielsweise um ein 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 dem Befehl `cd` zu dem in Schritt 1 erstellten Verzeichnis.
4. Führen Sei die Datei `SetupConfig.exe` aus, um die Parameterdatei `Setup.ini` zu erstellen. Beim erstmaligen Ausführen der Datei `SetupConfig.exe`, müssen Sie für alle Parameter Werte eingeben. Danach können Sie die Datei `SetupConfig.exe` bei Bedarf erneut ausführen, um die 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 **Notebook Extension Policy Servers**. Dabei kann es sich um einen NetBIOS-Namen wie `IHRSERVER` oder einen vollständig qualifizierten Domänennamen wie `IhrServer.IhreFirma.com` handeln.
   - **Benutzername** – der Benutzername eines Benutzers mit Administratorrechten auf den Computern, die das Notebook Extension 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. `IHREFIRMA\JerryAdmin`.
   - **Passwort** – das zum Benutzernamen gehörende Passwort. Dieses müssen Sie zweimal eingeben, um es zu bestätigen.
5. Führen Sie auf dem Benutzercomputer die Datei `StartInstall.exe` aus. Beispiel: `\\IhrServer\DPNEDeploy\StartInstall`. Mithilfe der Anmeldedaten (Benutzername und Passwort), die in der Datei `Setup.ini` angegeben sind, wird anschließend im Hintergrund mit geringer Priorität die Datei `Setup.exe` ausgeführt. Dies kann im Rahmen eines Anmeldescripts erfolgen. Beachten Sie, dass dafür kein Startscript verwendet werden kann, da das Computerkonto nicht über ausreichende Netzwerkberechtigungen verfügt.

6. `Setup.exe` ermittelt, ob der Benutzercomputer Notebook Extension unterstützt. Informationen zu unterstützten Windows-Plattformen finden Sie in der Supportmatrix.
7. `Setup.exe` ermittelt, ob .NET Framework Version 2.0 SP1 installiert ist. Wenn dies nicht der Fall ist, wird es installiert. Danach muss möglicherweise ein Neustart des Computers durchgeführt werden.
8. `Setup.exe` ermittelt, ob Notebook Extension bereits installiert ist. Wenn dies nicht der Fall ist oder eine ältere Version installiert ist,wird Notebook Extension installiert.

HINWEIS:

Wenn in den Schritten 4 bis 7 Fehler auftreten, werden auf dem Notebook Extension Policy Server und im Anwendungsereignisprotokoll auf dem lokalen Computer entsprechende Nachrichten protokolliert.

Den Fortschritt der Agentenbereitstellung können Sie wie folgt über die Policy Server-Konsole von Agent überprüfen:

1. Melden Sie sich an der Notebook Extension Policy Server-Konsole an.
2. Wählen Sie im Navigationsbereich auf der linken Seite unter **Berichte** den Eintrag **Agentenbereitstellung** aus.

   Daraufhin wird eine Zusammenfassung des Fortschritts Ihrer Erstbereitstellung bis zu diesem Zeitpunkt angezeigt. Folgende Informationen sind enthalten:

   - Anzahl der Computer, die die Bereitstellung erfolgreich **abgeschlossen** haben.
   - 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 entsprechenden Bereitstellungsstatus anzuzeigen.

   Zu jedem Computer wird der aktuelle Status angezeigt. Wenn die Bereitstellung beispielsweise auf einem bestimmten Computer fehlgeschlagen ist, wird in der Spalte **Informationen** der aufgetretene Fehler angezeigt. Weitere Informationen zu einem Computer erhalten Sie, indem Sie auf dessen NETBIOS-Namen klicken.

Agenten aktualisieren

Wenn Sie den Notebook Extension-Server aktualisieren, funktionieren vorhandene Agenten, die die Vorversion von Notebook Extension verwenden, weiterhin wie

bisher. Sie können sie manuell oder mithilfe der Agentenaktualisierungsrichtlinie im Hintergrund aktualisieren.

Automatische Agentenaktualisierung mithilfe der Agentenaktualisierungsrichtlinie

Agenten können mithilfe der Agentenaktualisierungsrichtlinie des Policy Servers im Hintergrund aktualisiert werden. Das Installationspaket wird automatisch an alle verbundenen Clients verteilt und die Aktualisierung erfolgt völlig automatisch. Der Benutzer wird bei seiner Arbeit nicht unterbrochen.

1. Wählen Sie in der Policy Server-Konsole **Richtlinien -> Agentenaktualisierungsrichtlinie** aus.
2. Wenn Ihr Policy Server soeben aktualisiert wurde, wurde bei der Installation ein neues Agentenaktualisierungspaket hochgeladen. Diese neue Version ist in der Policy Server-Konsole noch nicht ausgewählt.

   Wählen Sie die neue Agentenversion aus, um die Version verfügbar zu machen.
3. Durch Anpassen der Drosselung können Sie die maximal zulässige Anzahl von Aktualisierungen pro Minute festlegen.
4. Klicken Sie auf **Agentenaktualisierungsrichtlinie speichern**.
5. Nun werden die Agenten automatisch auf die neueste Version aktualisiert. Auch die Cleanup-Agenten werden automatisch aktualisiert.

HINWEIS:

Mithilfe des folgenden Berichts können Sie den Fortschritt der Agentenaktualisierung überprüfen: "Agentenverteilung".

Manuelle Agentenaktualisierung

Um einen vorhandenen Notebook Extension-Agenten auf eine neuere Version zu aktualisieren, führen Sie die Standardinstallationsprozedur durch.

Bevor Sie den Agenten auf eine neuere Version aktualisieren, stellen Sie sicher, dass die Version des Agenten mit der Version des Notebook Extension Policy Servers kompatibel ist.

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf der Seite "Data Protector Notebook Extension installieren" des Assistenten auf **Agenten installieren**, um die Aktualisierung zu starten.
3. Befolgen Sie die angezeigten Anweisungen.
4. Bei der Installation wird die vorhandene Agenteninstallation erkannt und die Aktualisierung angeboten.
5. Befolgen Sie die angezeigten Anweisungen.

5 Unterstützung für Notebook Extension anfordern

In Notebook Extension ist ein Wartungsvertrag mit einjähriger Laufzeit enthalten. Dieser beinhaltet für Sie das Recht auf folgende Unterstützungsleistungen:

- Telefonische Unterstützung, direkter Kontakt zu einem Kundendiensttechniker.
- Aktualisierungen für die Notebook Extension-Server- und -Agentensoftware. Die jeweils aktuellen Versionen oder CD-ROM-Images können von der Website für Data Protector heruntergeladen werden. 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 Netzwerkressourcen und ermöglicht es Benutzern und Anwedungen auf diese Ressourcen zuzugreifen. Verzeichnisdienste dienen dazu, Ressourcen unabhängig vom physischen System zu benennen, zu beschreiben, zu finden, zu verwalten und auf sie zuzugreifen.

Agent Notebook Extension-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.

Anfangs-aktualisierung Notebook Extension schützt Dateien kontinuierlich, indem alle von Benutzern vorgenommenen Änderungen gespeichert werden. Nach dem Erstellen eines neuen Data Vaults durch einen Benutzer muss Notebook Extension zuerst eine Anfangsaktualisierung aller geschützte Dateien des Benutzers im Data Vault durchführen. Der Benutzer kann bestimmen, ob die Anfangsaktualisierung sofort oder im Hintergrund durchgeführt wird.

Benutzerkontroll-richtlinie Diese Richtlinie bestimmt, wieviel 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. Die jeweilige Kontrollstufe können Sie für jede umfassendere Notebook Extension-Richtlinie separat einstellen. 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. Zentral definierte Data Vaults werden von einem in der Data-Vault-Richtlinie festgelegten Computer bereinigt. Die Cleanup-Richtlinie gilt für alle Benutzer.

Continuous File Protection Continuous File Protection ist das Continuous Data Protection-Verfahren von Notebook Extension, bei dem 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 Notebook Extension 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 Ein Data Vault ist ein gemeinsam genutzter (freigegebener) Ordner auf einem Dateiserver, in dem Dateien gemäß einer Data Vault-Richtlinie gespeichert werden. Der Dateiserver muss das Windows-Dateifreigabeprotokoll (CIFS/SMB) unterstützen. 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 Notebook Extension gesichert wird. Die geschützten Dateitypen werden in den Continuous- und Open File Protection-Richtlinien definiert.

Konsole Über die browserbasierte Konsole definieren Sie Notebook Extension-Richtlinien zentral. Sie müssen jedoch Mitglied der Administratorengruppe sein.

Kopierichtlinie Mit Kopierichtlinien wird Folgendes definiert:

- Anzahl der Agenten, die gleichzeitig Dateien auf 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 Notebook Extension nur Informationen über die Änderungen in den Data Vault kopiert werden, wenn ein Benutzer eine von Notebook Extension im Continuous-Modus geschützte Datei ändert.

Nach der Installation von Notebook Extension muss eine Kopierichtlinie definiert werden, um eine Anfangsaktualisierung aller geschützten Dateien Ihrer Benutzer durchzuführen.

Local Repository

Beim Local Repository handelt es sich um einen sicheren Speicherort auf Agentencomputern, 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 des 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, könnten 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.

Policy Server Der Policy Server verwaltet die Notebook Extension-Richtlinien zentral. Außerdem sammelt er Statusinformationen von den Agenten und stellt Berichte über deren Bereitstellung und Betrieb bereit.

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

Stichwortverzeichnis

H

I

K

L

N

P

R

S

T

U

V

W

Z