HP Data Protector for PCs 7.0 Guida all'installazione e amministrazione

Codice prodotto HP: n/d
Pubblicato: Giugno 2011
Edizione: Prima

Sommario

Informazioni sulla presente guida

La presente guida contiene informazioni su:

- Installazione di HP Data Protector for PCs
- Configurazione dei criteri per HP Data Protector for PCs
- Software agente HP Data Protector for PCs su desktop e portatili
- Determinazione del numero di Agenti che possono essere supportati
- Come ottenere supporto per Data Protector for PCs

Destinatari

La presente guida è destinata agli amministratori e serve per installare e configurare HP Data Protector for PCs. È utile conoscere:

- l'amministrazione di Windows

Convenzioni e simboli usati nel documento

Convenzione	Elemento
Testo in blu: "Informazioni sulla presente guida" (pagina 5)	Collegamenti a riferimenti incrociati e indirizzi di posta elettronica
Testo sottolineato, in blu: http://www.hp.com	indirizzi di siti web
Testo in **grassetto**	• Tasti da premere • Testo da inserire in un elemento dell'interfaccia utente grafica • Elementi dell'interfaccia utente grafica su cui fare clic o da selezionare, quali menu ed elementi di elenchi, pulsanti, schede e caselle di selezione
Testo in *corsivo*	Enfasi al testo

Convenzione	Elemento
Testo con `spaziatura fissa`	• Nomi di file e directory • Output dal sistema • Codice • Comandi, argomenti dei comandi e valori degli argomenti
Testo con *`spaziatura fissa, in corsivo`*	• Variabili del codice • Variabili dei comandi
Testo con **`spaziatura fissa, in grassetto`**	Testo enfatizzato con spaziatura fissa

IMPORTANTE: Fornisce chiarimenti o istruzioni specifiche.

NOTA: Fornisce informazioni aggiuntive.

Informazioni generali

Informazioni generali su Data Protector for PCs sono disponibili in http://www.hp.com/go/dataprotector.

Supporto tecnico HP

Per informazioni sul supporto tecnico nel mondo, visitare il sito di supporto HP:

http://www.hp.com/support

Prima di contattare HP, si prega di reperire le seguenti informazioni:

- Nomi e numeri del modello del prodotto
- Numero di registrazione presso il supporto tecnico (se applicabile)
- Numeri di serie del prodotto
- Messaggi di errore
- Tipo di sistema operativo e livello della revisione
- Quesiti specifici

Servizio in abbonamento

HP raccomanda di registrare il prodotto sul sito web Subscribers Choice per aziende:

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

Dopo la registrazione si riceveranno notifiche per posta elettronica relative a miglioramenti apportati ai prodotti, versioni nuove dei driver, aggiornamenti del firmware e su altre risorse per i prodotti.

Siti web di HP

Per ulteriori informazioni, visitare i seguenti siti web di HP:

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

Commenti sulla documentazione

HP è lieta di ricevere commenti.

Per inviare commenti e suggerimenti sulla documentazione dei prodotti si prega di inviare un messaggio al seguente indirizzo: **DP.DocFeedback@hp.com**. Tutti i materiali inviati diventano di proprietà di HP.

1 Panoramica e prerequisiti

Panoramica di Data Protector for PCs

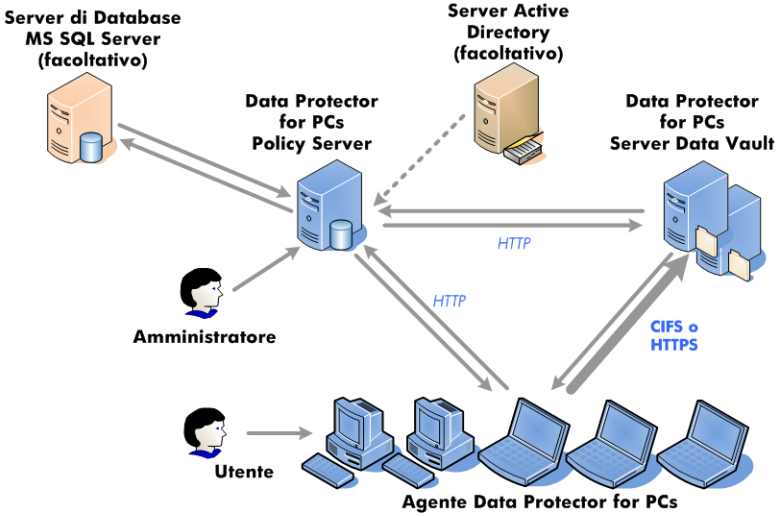
HP Data Protector for PCs consta di due componenti principali, il Policy Server e gli agenti. Policy Server viene eseguito su un server Windows, fare riferimento alla matrice del supporto per le versioni supportate (https://h20230.www2.hp.com/selfsolve/manuals). Gli agenti vengono eseguiti in background su ciascun desktop o portatile.

Policy Server può anche accedere a gruppi e unità organizzative contenute in un server Active Directory.

Nei Data Vault viene eseguito il backup dei dati degli utenti. Il server Data Vault deve essere separato dal Policy Server. Se anziché utilizzare i Data Vault Web consigliati, si utilizzano Data Vault sulla condivisione di file Windows, questi si trovano su una più condivisioni di file Windows o su file server.

L'architettura di Data Protector for PCs viene presentata nello schema seguente:

Figura 1 Data Protector for PCs architettura



Diversi criteri controllano per quali file viene eseguito il backup da desktop e portatili e dove vengono conservati i backup. Questi criteri sono definiti nella console del Policy Server. I criteri sono quindi distribuiti automaticamente agli agenti, usando il protocollo SOAP su HTTP porta 80. I criteri vengono conservati sul Policy Server.

Questi criteri vengono applicati dagli agenti. Quando un utente modifica un file dati protetto come stabilito nei criteri, sul disco rigido locale del desktop/portatile viene creata una versione precedente e i cambiamenti del file sono compressi e copiati su tutti i Data Vault applicabili.

Quando si esegue il backup dei file, l'agente invia al Policy Server una notifica che contiene una cronologia dell'audit dei cambiamenti ai file apportati dagli utenti. Inoltre, ogni agente invia periodicamente informazioni sull'integrità al Policy Server. È possibile generare report di tali dati utilizzando la console del Policy Server.

I Data Vault sono conservati sul server Data Vault. I dati dei client vengono copiati nei Data Vault utilizzando due protocolli differenti: CIFS (per Data Vault sulle condivisioni di file Windows) o HTTP (per i Data Vault sul web).

Il server Data Vault deve trovarsi su un sistema separato dal Policy Server. Per HTTPS, il software del server Data Vault Web viene eseguito su di esso, insieme al software Cleanup di Data Protector for PCs. Per i Data Vault sulle condivisioni di file Windows, vi viene installato solo il software Cleanup.

Se si utilizza Active Directory, è possibile configurare il Policy Server in modo che effettui l'accesso a gruppi e unità organizzative. I Data Vault possono essere assegnati agli utenti in base al gruppo o all'unità organizzativa di appartenenza. Nei report è anche possibile selezionare gli utenti in base alla loro appartenenza.

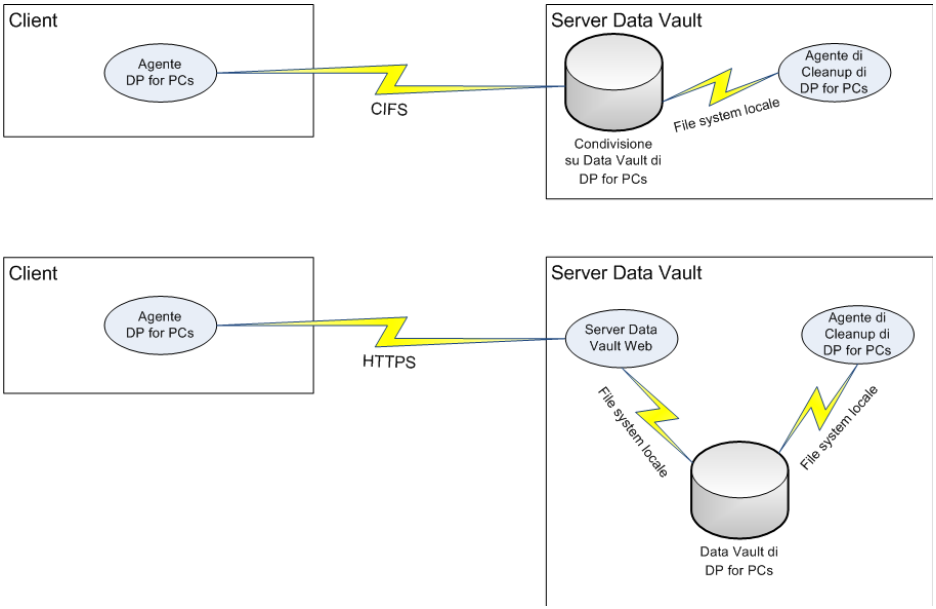
Data Vault

Esistono due tipi di Data Vault per Data Protector for PCs:

- Data Vault Web che utilizzano il protocollo HTTPS. Forniscono il livello migliore di protezione e offrono la migliore velocità effettiva in ambienti a elevata latenza, e pertanto sono raccomandata.
- Data Vault su condivisioni di file Windows, basati sul protocollo CIFS, usato nelle versioni precedenti di Data Protector for PCs.

I dati hanno la medesima struttura su entrambi i tipi di Data Vault, pertanto è possibile convertire Data Vault sulle condivisioni di file Windows in Data Vault Web.

Figura 2 Confronto tra la una condivisione di file Windows e Data Vault Web



Gestione dei certificati

Per i Data Vault Web è obbligatorio utilizzare l'SSL. Il tipo di certificato viene determinato durante l'installazione del Data Vault Web. Per fornire un prodotto che possa essere subito pronto, ad esempio poterlo valutare, è possibile installare il server Web Data Vault con un certificato autofirmato. Non è sicuro come un certificato emesso da un'autorità attendibile (CA). Per avere una protezione completa, è necessario importare un certificato per il server Data Vault firmato da un'autorità attendibile all'interno del proprio ambiente da aggiungere al componente server.

Certificati autofirmati

Quando si crea un criterio di Data Vaultè possibile definire se è consentito un certificato autofirmato. In questo caso non è necessaria alcuna azione sul lato agente. Un certificato autofirmato emesso dall'installazione è limitato a 20 anni.

Certificati importati

La procedura di importazione prevede un solo file in formato PEM che contenga sia la chiave privata che il certificato corrispondente che comprende la chiave pubblica. Si noti che il file viene copiato nella directory della configurazione server Data Vault Web nello stato in cui è. In relazione alla procedura utilizzata per la creazione del file del certificato, esso potrebbe essere crittografato. In questo caso, il processo del servizio Windows responsabile dell'esecuzione del server Data Vault Web rilascerà un prompt interattivo per ricevere la password di decrittografia. Questo accade nel corso dell'installazione e anche ogni volta che il servizio viene riavviato in futuro, ad esempio

dopo il riavvio del sistema. Pur essendo possibile aggiungere questa password manualmente al file di configurazione del server Web per evitare di ricevere il prompt, il processo di installazione non supporta questa funzione. Non è consigliabile avere un file certificato crittografato e archiviare la password in un file la cui posizione è molto vicina al file certificato.

NOTA:
La locuzione "autorità attendibile" implica che i client nei quali è in esecuzione l'agente devono considerare questa CA affidabile e accettare i certificati firmati da questa autorità. Si ipotizza che i Windows Certificate Store dei client siano già stati impostati correttamente con l'aggiunta del certificato della CA e di ulteriori potenziali certificati nelle rispettive linee. L'agente non comprende eventuali meccanismi per la creazione di questa attendibilità. Si affida ai meccanismi di Windows.

Scambio del certificato

È possibile scambiare il certificato sul server Data Vault Web dopo l'installazione usando l'utilità `DvConfig` descritta nel paragrafo CLI "Configurazione delle opzioni per i Data Vault Web da CLI (DvConfig)" (pagina 21). Ad esempio, è possibile riconfigurare un'installazione che era stata inizialmente impostata con un certificato autofirmato in modo che utilizzi un certificato importato.

Panoramica dell'installazione di Data Protector for PCs

NOTA: Se si sta eseguendo l'aggiornamento di un'installazione di Data Protector for PCs, fare riferimento a "Aggiornamento di Data Protector for PCs" (pagina 42).

L'installazione di Data Protector for PCs viene eseguita in tre fasi:

1. **Installazione di Data Protector for PCs Policy Server.**

   Vedere "Installazione di Data Protector for PCs Policy Server" (pagina 14).

2. **Installare il software per il server Data Vault Web di Data Protector for PCs.**

   Fare riferimento a "Installazione, configurazione e manutenzione del server Data Vault Web." (pagina 18).

3. **Configurazione dei criteri di protezione.**

   Vedere "Configurazione dei criteri di protezione di Data Protector for PCs" (pagina 23).

4. **Installazione degli agenti di Data Protector for PCs su portatili e desktop.**

   Vedere "Installazione degli agenti Data Protector for PCs" (pagina 37).

Prerequisiti

Policy Server

Per i sistemi operativi supportati, fare riferimento alla matrice del supporto.

NOTA: *Installazione su sistemi operativi Windows 2003 a 64-bit:* nei sistemi operativi Windows a 64-bit, Policy Server viene eseguito in modalità compatibilità a 32-bit. Ciò significa che IIS (Internet Information Services) deve essere eseguito in modalità a 32-bit. In caso contrario, questa condizione viene rilevata durante il controllo dei prerequisiti in fase di installazione. Il sistema consente di impostare la modalità a 32-bit per IIS. Se sul server sono presenti altre applicazioni per il web per le quali IIS deve essere in modalità a 64-bit (come ad esempio Microsoft Exchange con Web mail Outlook Web Access), non sarà possibile installare Policy Server sul server in esame. Quanto sopra non si applica all'installazione di Policy Server su Windows 2008.

Sul server devono essere installati:

- Internet Information Services 6.0, 7.0, 7.5 o versione successiva con supporto per le applicazioni ASP.NET.

  Per Windows 2003, IIS 6.0 è un prerequisito e deve essere installato prima di poter installare Policy Server. Per Windows 2008, Data Protector for PCs consente di installare IIS 7.0 e 7.5, se non ancora installati.

- Microsoft ASP.NET 2.0

Sul server devono essere installati anche i seguenti elementi:

- Microsoft Installer 3.1 o versione successiva (richiesto per .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 o versione successiva. La versione 2.0 SP1 viene installata da una procedura guidata.
- Microsoft SQL Express (se non è già presente un'altra versione di SQL)

Inoltre per Internet Information Services 7.0 e 7.5 soltanto, sono necessari i seguenti componenti IIS. Se non fossero installati, la procedura guidata consente di procedere alla loro installazione:

- IIS Static Content Web Server, richiesto per poter elaborare file html statici, documenti e immagini
- IIS ASP.NET, richiesto per la distribuzione di ASP.NET 2.0 e .NET Framework
- IIS Security, richiesto per usare l'autenticazione integrata di Windows per la console di Policy Server.
- IIS 6 Management Compatibility, per consentire di avere la stessa configurazione per IIS 6 e IIS 7

Database

Data Protector for PCs deve poter accedere a un database di Microsoft SQL Server. Vedere la matrice del supporto per le versioni supportate.

Utilizzando Microsoft Enterprise Manager è possibile verificare (e modificare) la modalità di autenticazione dell'installazione di SQL Server:

1. Fare clic con il tasto destro sull'istanza di SQL Server, selezionare **Proprietà** e fare clic sulla scheda **Protezione**.
2. Deve essere già stata selezionata l'opzione **SQL Server e Windows** (e non l'opzione **Solo Windows**). In caso contrario, selezionarla e fare clic su **OK**.

Altrimenti, durante l'installazione di Data Protector for PCs, è possibile installare un'istanza di SQL Server Express Edition di Microsoft.

Server Data Vault Web di Data Protector for PCs

- Il server Data Vault Web deve trovarsi su un sistema separato dal Policy Server. (Può anche essere installato sullo stesso sistema, ma questo tipo di installazione è idonea solo per poter valutare il prodotto).
- È necessario installare l'ambiente Java Runtime versione 1.6 o successiva.
- Le variabili `JAVA_HOME` e `JRE_HOME` devono puntare alla directory di installazione di Java Runtime.

Agenti Data Protector for PCs

Il software agente di Data Protector for PCs può essere installato nei desktop e nei portatili degli utenti con Windows. Per le piattaforme supportate, fare riferimento alla matrice del supporto.

2 Installazione di Data Protector for PCs Policy Server

NOTA: È possibile aggiornare un'installazione esistente di Policy Server per Data Protector for PCs a una versione più recente seguendo la procedura standard per l'installazione. Fare riferimento a "Aggiornamento del Policy Server" (pagina 42) per maggiori informazioni.

Installazione rapida

Fare riferimento a "Policy Server" (pagina 12) per i requisiti di Policy Server per Data Protector for PCs.

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Se la procedura guidata di installazione non viene avviata automaticamente, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione.
2. Seguire le istruzioni riportate sullo schermo.
3. Data Protector for PCs Policy Server deve poter accedere a un database di Microsoft SQL Server. Selezionare **Usa l'istanza presente di Data Protector for PCs presente di Microsoft SQL Server Express** o fare clic su **Usa un'istanza presente di Microsoft SQL Server** . Se si sceglie di utilizzare un SQL Server esistente, è necessario specificare la stringa di connessione del server del database e le credenziali di un account che disponga di credenziali sufficienti per creare un nuovo database.
4. Fare clic su **Installa** nella pagina **Installa Data Protector for PCs Policy Server** della procedura guidata per iniziare l'installazione.
5. Una volta completata l'installazione, fare clic su **Avanti** . A questo punto è possibile eseguire la console Data Protector for PCs Policy Server.
6. Installare il server Data Vault Web su un sistema separato. Fare clic su **Installa Data Vault** nella schermata principale dell'installazione.

NOTA: Nel corso dell'installazione, il software Cleanup viene sempre installato insieme al software server Data Vault Web. Per i server Data Vault con Data Vault su una condivisione di file Windows, si raccomanda di eseguire l'installazione in locale, sul Data Vault, per ottimizzare le prestazioni.

Istruzioni dettagliate per l'installazione

NOTA:
Solo per Windows 2003 server: È possibile installare Data Protector for PCs Policy Server da un CD ROM condiviso in rete o da una condivisione di file di rete solo se i Criteri di protezione runtime di .NET 2.0 Framework Runtime Security Policy per questo server sono impostati su *Attendibilità totale* per la zona di protezione della Intranet locale. Se il server non dispone di una unità CD ROM locale, modificare i Criteri di protezione runtime per la Zona di protezione della Intranet locale su *Attendibilità totale* utilizzando lo strumento di configurazione di .NET Framework 2.0 negli Strumenti di amministrazione o copiare la cartella del server dal CD al disco locale sul server.

È necessario avere effettuato l'accesso con un account con privilegi "amministrativi" per l'installazione di Policy Server di Data Protector for PCs.

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Se la procedura guidata di installazione non viene avviata automaticamente, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione.
2. Fare clic su **Installa Policy Server**.

   Se chiesto, scegliere **Apri** (o **Esegui**) per aprire il programma dalla posizione corrente invece di **Salva l'applicazione su disco**.
3. Data Protector for PCs Policy Server richiede .NET Framework 2.0 SP1. Se ancora non è stato installato, verrà chiesto se si desidera installarlo dal CD ROM.

   L'installazione richiede Windows Installer 3.1 o versione successiva, pertanto, se necessario, verrà chiesto di installare Windows Installer 3.1 dal CD.
4. La procedura guidata di installazione verifica se gli altri elementi prerequisiti sono installati:
   - Internet Information Services (IIS)
   - ASP.NET 2.0

   Se uno di questi non è installato, fare clic sul prerequisito nell'elenco per i dettagli su come eseguire l'installazione.

   Fare clic su **Avanti**.
5. Installare Microsoft SQL Server.

   Per utilizzare un'istanza esistente di Microsoft SQL Server:

   a. Fare clic su **Utilizza un'istanza esistente di Microsoft SQL Server**.

b. Nel campo **Server database**, inserire la stringa di connessione per il server database esistente.

c. Nei campi **Accesso** e **Password**, inserire le credenziali di un account che disponga di credenziali sufficienti per creare un nuovo database. Di norma è l'account "sa".

d. Fare clic su **Avanti**. Le informazioni di connessione inserite verranno utilizzate per eseguire un test di connessione al server database esistente. Se la connessione viene stabilita, la procedura guidata continua con il passaggio 6.

Per installare l'istanza Data Protector for PCs di Microsoft SQL Server Express Edition:

a. Selezionare **Installa l'istanza DataProtectorNE di Microsoft SQL Server Express** e fare clic su **Avanti**.

b. Fare clic su **Installa** per installare l'istanza di Microsoft SQL Server 2005 Express Edition denominata "DataProtectorNE". Completata l'installazione, fare clic su **Avanti**.

6. Installare il software Data Protector for PCs Policy Server.

   a. Nella schermata iniziale, fare clic su **Avanti** per iniziare l'installazione.

   - La console di Policy Server di Data Protector for PCs verrà installata come applicazione Web nella directory virtuale `C:\Inetpub\wwwroot\dpnepolicy`.
   - Il servizio Web di Data Protector for PCs verrà installato in `C:\Inetpub\wwwroot\dpnepolicyservice`.

   Entrambi utilizzano il protocollo HTTP sulla porta 80.

   b. Fare clic su **Chiudi** e **Avanti** una volta completata l'installazione di Policy Server.

7. A questo punto è necessario installare il programma Cleanup. Fare clic su **Installa** per iniziare l'installazione.

8. Una volta completata l'installazione di Cleanup, fare clic su **Avanti** .

   Data Protector for PCs può essere amministrato centralmente dalla console di Data Protector for PCs Policy Server. Poiché la console è basata sul browser, è possibile gestire Data Protector for PCs da un qualsiasi computer in grado di stabilire una connessione del browser con il Policy Server (utilizzando HTTP e la porta 80).

   Per eseguire la console di Data Protector for PCs Policy Server da un browser sul Policy Server, lasciare la casella di controllo **Esegui console di Policy Server** selezionata e fare clic su **Fine**.

NOTA: Il software Cleanup viene installato nel corso dell'installazione di Policy Server. Si raccomanda di installarlo nei Data Vault per ottimizzare le prestazioni.

NOTA:
Impostazioni browser per la console di Policy Server: in caso di problemi di visualizzazione delle pagine della console di Policy Server nel browser, verificare le impostazioni di protezione del browser. La Console richiede quanto segue:

- JavaScript deve essere abilitato.
- Il blocco popup deve essere disabilitato per il sito web dpnepolicy.
- Le altre impostazioni di protezione devono essere modificate in relazione al browser e alla versione.

Installazione con Microsoft SharePoint: Una volta installato Policy Server su un server con Microsoft SharePoint in esecuzione, potrebbe essere visualizzato l'errore 404 "Impossibile trovare la pagina" quando si esegue la console di Policy Server. L'articolo della knowledge base di Microsoft disponibile su http://support.microsoft.com/kb/828810 descrive il problema e la soluzione. Si noti che questo problema si applica a tutte le applicazioni web ASP.NET e non solo a Policy Server.

Per eseguire il Policy Server su un server che utilizza SharePoint, è necessario procedere come segue:

1. Utilizzare gli strumenti di amministrazione di SharePoint per creare le esclusioni per le due applicazioni web di Policy Server: `dpnepolicy` e `dpnepolicyservice`.
2. Modificare i due file `web.config` di Policy Server (`dpnepolicy\web.config` e `dpnepolicyservice\web.config`) per aggiungere il codice XML `<httpHandlers>>` e `<trust>>` come descritto nell'articolo della knowledge base di Microsoft a cui si faceva riferimento in precedenza.

3 Installazione, configurazione e manutenzione del server Data Vault Web.

Installazione e configurazione server Data Vault Web

NOTA: Installare il server Data Vault Web su un sistema separato dal Policy Server. (Può anche essere installato sullo stesso sistema, ma questo tipo di installazione è idonea solo per poter valutare il prodotto).

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Se la procedura guidata di installazione non viene avviata automaticamente, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione.
2. Fare clic su **Installa Data Vault**.
3. Scegliere tra:
   - **Server Data Vault Web** (raccomandato). Anche il software Cleanup viene installato sul server.
   - **Software Cleanup per Data Vault sulla condivisione di file Windows**. Selezionare questa voce per utilizzare i Data Vault sulla condivisione di file Windows.

   Fare riferimento a "Data Vault" (pagina 9) per maggiori informazioni.
4. Seguire le istruzioni presentate sullo schermo per completare la fase di installazione.
5. Dopo avere ricevuto la licenza da Policy Server, se si sta installando un server Data Vault Web, è possibile iniziare a configurare il Data Vault Web.

   Nella schermata Impostazioni server, immettere il nome di dominio completo (FQDN) e la porta SSL del server. È necessario utilizzare lo stesso FQDN quando si configura il criterio di Dat Vault Web sul Policy Server. Il nome deve essere risolvibile da tutti i sistemi client, altrimenti non sarà possibile eseguire il backup di alcuni di questi clienti sui Data Vault presenti in questo server.
6. Nella schermata Impostazioni certificato è necessario scegliere tra:
   - Importazione di un certificato SSL esistente emesso da un'autorità attendibile (CA). Questa è la scelta consigliata e offre il livello più elevato di protezione.
   - Creazione di un certificato SSL autofirmato. Questa opzione offre un livello minore di protezione e deve essere usata per valutare il prodotto.

NOTA: È possibile scambiare il certificato sul server Data Vault Web in qualsiasi momento usando l'utilità `DvConfig`. Questa scelta implica la necessità di riconfigurare un'installazione con un certificato autofirmato per utilizzare un certificato importato. Fare riferimento a "Configurazione delle opzioni per i Data Vault Web da CLI (DvConfig)" (pagina 21).

7. La schermata successiva chiede di fornire i nomi di due tipi di utente del server Data Vault Web:
   - **Utente con privilegi amministrativi**— che si occupa di attività di tipo amministrativo quali la creazione e l'eliminazione di Data Vault e la migrazione dei dati di backup dei client.
   - **Utente per il backup**—che esegue operazioni tipiche dell'utente finale quali il backup e il ripristino di file.

   Si tratta di utenti specifici del server Data Vault Web di Data Protector for PCs. Per la creazione o l'eliminazione di Data Vault Web per questo server è necessario immettere i dettagli relativi a ciascun utente.

   NOTA: La password deve essere composta da almeno 8 caratteri.

8. Fare clic su **Avanti** e poi su **Fine** per completare l'installazione e la configurazione del server Data Vault Web e l'installazione del software Cleanup.

Manutenzione dei Data Vault Web

1. Nella pagina criteri di Data Vault, immettere il nome completo del dominio del server e la porta SSL, e le credenziali dell'account Utente per il backup. Fare clic su **Configura Data Vault**.
2. Inviare le credenziali account Utente con privilegi amministrativi per visualizzare la pagina Manutenzione server Data Vault Web.

   Da qui è possibile selezionare o cancellare i Data Vault Web esistenti. È anche possibile aggiungere un nuovo Data Vault.

   NOTA: È possibile selezionare un Data Vault esistente se non è al momento connesso a un altro criterio di Data Vault.

3. Fare attenzione a salvare il criterio di Data Vault facendo clic su **Salva** in fondo alla pagina.
4. Se è stato aggiunto un nuovo Data Vault, è possibile testare l'esistenza e la corretta configurazione del Vault.

Migrazione dei dati da un Data Vault sulla condivisone di file Windows a un Data Vault Web:

Il layout dei dati in un Data Vault è lo stesso sia per i Data Vault sulle condivisioni di file Windows che per i Data Vault Web HTTPS. In altre parole è possibile eseguire la migrazione dei dati dai Data Vault esistenti di DPNE 6.x ai nuovi Data Vault Web.

NOTA: La migrazione dei dati può essere eseguita solo per i Data Vault che appartengono a uno stesso Policy Server o che condividono la medesima password di crittografia.

Per la migrazione dei dati sono possibili due scenari:

- Utilizzare lo stesso sistema per ospitare il Data Vault Web.

  NOTA: Non è supportato l'accesso alla stessa directory in parallelo tramite una condivisione di file WIndows e un Data Vault Web.

- Spostare l'intero Data Vault su un altro sistema.

In entrambi i casi il server Data Vault Web deve essere installato in locale sul sistema nel quale devono essere residenti i dati.

Per migrare i dati da un Data Vault sulla condivisone di file Windows a un Data Vault sul web:

NOTA:

- Eseguire la migrazione al di fuori dell'orario di lavoro per contenere gli effetti sui backup in esecuzione.
- Controllare in gestione attività di Windows che `DPNECleanup.exe` non sia in esecuzione.
- Controllare i criteri di Cleanup sul Policy Server per assicurarsi che l'esecuzione di `DPNECLeanup.exe` non sia pianificata per il periodo previsto per la migrazione

1. Installare il server Data Vault Web e aggiornare Policy Server e gli agenti alla versione 7.0. Assicurarsi che tutti gli agenti abbiano eseguito il riavvio dopo l'installazione della 7.0, poiché solo dopo questa operazione sarà possibile iniziare a eseguire il backup dei dati sul Data Vault sul web.
2. Disabilitare i criteri condivisione di file Windows dalla pagina criteri di Data Vault, in modo che agenti non copino più i dati sul Data Vault.
3. Se si utilizzerà la stessa directory per il Data Vault Web, interrompere la condivisione della directory tramite CIFS.
4. Se il Data Vault Web si trova su un server diverso dal Data Vault sulla condivisione di file Windows, i dati devono essere copiati su tale computer in un percorso di cartella che non abbia più di 67 caratteri. Se il data Vault è residente sullo stesso

server, non è necessario copiare i dati nella nuova posizione, a meno che ciò sia fatto intenzionalmente per altre ragioni.

5. Prima di creare il nuovo Data Vault Web, definire il comportamento del processo iniziale di aggiornamento. È possibile ignorare l'aggiornamento iniziale se tutti gli agenti hanno eseguito un aggiornamento iniziale, in modo tale che il backup dei dati sia già completo sul Data Vault esistente. L'opzione per ignorare l'aggiornamento iniziale non fa parte di un criterio di Data Vault, ma dei Criteri di copia a cui fa riferimento. Assicurarsi che sia presente un criterio di Data Vault con l'opzione corretta selezionata (ovvero, con "aggiornamento iniziale" non selezionato e le impostazioni corrette per limitazione e pianificazione). Creare un nuovo criterio di copia specifico, oppure modificare un criterio esistente (in questo caso, ciò si rifletterà su tutti i criteri di Data Vault che fanno riferimento al criterio di copia).
6. Creare e salvare i criteri Data Vault per il Data Vault Web. Quando si crea un nuovo Data Vault Web, è necessario fornire il percorso della cartella, e in questo caso si tratta del percorso in cui si trovano i dati del Data Vault sulla condivisione di file Windows dei quali si sta eseguendo la migrazione. Selezionare i criteri di copia creati nel passaggio 5. Impostare le opzioni per il criterio di Data Vault in modo che siano le identiche al criterio di Data Vault sulla condivisione di file Windows (quali ad esempio le impostazioni di rete, le impostazioni di Active Directory).
7. Quando si è certi che gli agenti stiano completando il backup dei file sul nuovo Data Vault Web, cancellare il criterio originale di Data Vault sulla condivisione di file Windows.

Dopo avere salvato il criterio, gli agenti riprendono la copia dei loro dati sul nuovo Data Vault Web usando il protocollo HTTPS.

Configurazione delle opzioni per i Data Vault Web da CLI (DvConfig)

Utilizzando questa utilità da CLI è possibile modificare i parametri di configurazione del Data Vault Web, quali ad esempio gli utenti per il backup e con privilegi amministrativi e le relative password, importare un certificato nuovo, modificare la porta SSL, e creare un nuovo certificato autofirmato.

Prima di modificare i parametri, è necessario arrestare il server Data Vault Web arrestando il servizio di Windows server Data Vault di HP Data Protector for PCs.

Dopo avere apportato le modifiche, riavviare il servizio Data Vault Web. Gli eventuali criteri aggiornati saranno distribuiti nuovamente agli agenti.

NOTA: Se si utilizza `DvConfig` per modificare la porta SSL oppure il nome o la password dell'utente per il backup sul server Data Vault Web, assicurarsi di modificare i relativi criteri di Data Vault sul Policy Server in modo che vi sia corrispondenza.

Utilizzo:

`DvConfig [-adminUser login:password -backupUser login:password] [-h] [-i certfile | -s hostname] [-p port] [-v]`

`-adminUser login:password`
Imposta le credenziali dell'account DvAdmin. Se non viene fornito un'accesso o una password, utilizzare quella predefinita "DvAdmin".

`-adminUser login:password`
Imposta le credenziali dell'account DvBackup. Se non viene fornito un'accesso o una password, utilizzare quella predefinita "DvBackup".

`–h`
Stampa questo mesdsaggio.

-i *certfile*
Importa un certificato esistente.

`-p port`Imposta la porta SSL.

`–s hostname`
Crea un certificato autofirmato per il nome dominio completo.

`–v`
Stampa le informazioni sulla versione ed esce.

4 Configurazione dei criteri di protezione di Data Protector for PCs

Configurazione iniziale dopo l'installazione di Data Protector for PCs

Una volta completata l'installazione di Data Protector for PCs, nella console di Policy Server viene visualizzata la finestra di Configurazione iniziale. Prima di poter configurare i criteri per Data Protector for PCs, è necessario completare due passaggi per la configurazione:

1. **Definire o importare una password di crittografia.**

   Per garantire la protezione, si deve definire una password di crittografia prima di poterla utilizzare Data Protector for PCs. In questo modo si garantisce che tutti i file sono crittografati nel computer dell'utente e che vengono crittografati qaundo sono trasmessi in rete. La stessa password viene usata per crittografare i file da tutti gli utenti e per tutti i Data Vault configurati a livello centrale.

   - Un Data Vault definito a livello centrale (definito tramite la console di Policy Server) usa sempre la crittografia in relazione alla password di crittografia per Data Protector for PCs.
   - Con i Data Vault definiti a livello centrale (definiti dagli utenti utilizzando i propri computer), gli utenti possono scegliere se utilizzare la crittografia o meno e scegliere le password desiderate.

   Quando si installa Data Protector for PCs per la prima volta, per poter proseguire è necessario **generare** o **importare** una password. Dopo avere generato una password, per la propria sicurezza, **esportare** la password. In questo modo viene salvata in una posizione protetta. Può essere importata successivamente.

   Fare clic su **Imposta i criteri di crittografia** per gestire la password e seguire le istruzioni nella finestra.

   NOTA: Non è possibile cambiare password dopo averla generata o importata.

2. **Licenza Data Protector for PCs.**

   Se si sta valutando Data Protector for PCs, è possibile utilizzarlo per 60 giorni per proteggere un numero di utenti illimitato senza che sia necessario avere un'ulteriore licenza. Quando si acquista Data Protector for PCs, è necessario visitare HP License Key Delivery Service all'indirizzo https://webware.hp.com/welcome.asp per scaricare il codice di licenza che è possibile utilizzare. È possibile acquistare le seguenti licenze

   - TA032AA o TA032AAE per 100 agenti
   - TA033AA o TA033AAE per 1000 agenti

- TA036AA o TA036AAE per 100 agenti oltre a HP Data Protector Starter Pack Windows (B6961BA o B6961BAE)

Prima del termine del periodo di valutazione è necessario immettere un codice di licenza permanente. In caso contrario, allo scadere dei 60 giorni, gli agenti non saranno più in grado di copiare i dati sui Local Repository o Data Vault. Tuttavia, è ancora possibile ripristinare le versioni dei file protetti in precedenza.

Fare clic su **Gestione licenze** per gestire le licenze, quindi **Immettere un codice di licenza per gli utenti di Data Protector for PCs**. Seguire le istruzioni nella finestra.

NOTA: Le licenze vengono distribuite agli agenti quando vengono installati.

Una volta completate le fasi della configurazione, è disponibile la versione completamente funzionante della console di Policy Server. Se si è installato Data Protector for PCs, configurare gli altri elementi di Data Protector for PCs nell'ordine specificato nella sezione successiva.

Prima configurazione

Data Protector for PCs viene fornito con criteri preconfigurati che sono sufficienti per la maggior parte delle organizzazioni. Si raccomanda di configurare prima i Data Vault, i criteri di copia e di protezione file e poi di procedere all'installazione del software agente di Data Protector for PCs sui desktop e sui portatili degli utenti.

NOTA: Invece di configurare criteri nuovi, è possibile modificare i criteri preconfigurati disponibili in Data Protector for PCs. È sufficiente selezionare **Modifica criterio esistente** invece di **Crea nuovo criterio** in qualsiasi fase.

I criteri di protezione per l'installazione vengono configurati dalla console di Policy Server. I criteri definiti a livello centrale vengono distribuiti a tutti gli agenti di Data Protector for PCs e vengono eseguiti sui desktop e portatili degli utenti.

1. Eseguire la console di Policy Server di Data Protector for PCs al termine della procedura di installazione o in qualsiasi altro momento dal browser utilizzando l'URL:

   `http://`*`policyserver`*`/dpnepolicy/`

   dove *`policyserver`* è il nome del Policy Server di Data Protector for PCs. È necessario eseguire l'accesso al server come "amministratore".

2. **Configurazione dei criteri di Data Vault**.

   I criteri di Data Vault impostano la destinazione (un Data Vault Web o una condivisione di file Windows) per il backup continuo di file degli utenti protetti da criteri. Quando viene modificato un file, viene eseguito automaticamente, su una o più destinazioni, il backup della versione precedente e del file modificato. A ogni gruppo di utenti può essere assegnato uno o più Data Vault. Ad esempio, è possibile

definire un criterio di Data Vault denominato *Vendite* e assegnarlo al gruppo di utenti *Dallas.Vendite*, *San Francisco.Vendite*, *Chicago.Vendite* e *Atlanta.Vendite*.

- Un Data Vault definito a livello centrale (definito tramite la console di Policy Server) usa sempre la crittografia in relazione alla password di crittografia per Data Protector for PCs.
- Con i Data Vaults definiti a livello centrale (definiti dagli utenti utilizzando i propri agenti), gli utenti possono scegliere se utilizzare la crittografia o meno e scegliere le password desiderate.

NOTA: *Requisito per tutti i Data Vault:*

Data Protector for PCs imposterà le autorizzazioni di accesso (ACL) per i file di backup del file server in modo che siano le stesse del file originale. Questo significa che gli utenti possono recuperare i file di backup solo se possono accedere ai file originali sui propri computer.

Requisito per i Data Vault sulle condivisioni di file Windows:

Se si utilizzando Data Vault standard sulle condivisioni di file Windows, le condivisioni devono trovarsi su un server file Windows, e non è necessario che sia la stessa macchina di Policy Server. Tuttavia, se si sta valutando Data Protector for PCs con un ridotto numero di agenti installati, potrebbe essere utile avere file server di Policy Server e Data Vault sullo stesso computer.

Per creare un criterio Data Vault:

a. Fare clic su **Criteri > Data Vault > Criteri di Data Vault** nel pannello di navigazione di sinistra.

b. Fare clic su **Crea un nuovo criterio di Data Vault**.

c. Seguire le istruzioni nella finestra. Il processo è differente in relazione al tipo di Data Vault selezionato: basato sul web o condivisione di file Windows.

NOTA: Quando si crea un Data Vault, il percorso della cartella o della condivisione non deve superare 66 caratteri.

Buone prassi:

Per il momento lasciare il criterio di copia impostato su Predefinito.

Per eseguire il Cleanup per i Data Vault su condivisioni di file Windows:

- Se il Data Vault si trova su questo Policy Server, conservare l'impostazione predefinita per il nome di questo computer.
- Se il Data Vault si trova su un file server diverso, installare il software di Cleanup per i Data Vault e specificare che il computer su cui è stata effettuata l'installazione è il computer di Cleanup.

3. **Configurazione dei criteri di copia**.

Criteri di copia consente di impostare un limite nel numero di client che possono copiare un Data Vault. Definisce inoltre gli aggiornamenti di Data Vault iniziali e pianificati per il backup continuo. A ogni criterio di copia può essere assegnato uno o più Data Vault.

I criteri di copia definiscono i seguenti elementi:

- Il numero di agenti che può copiare contemporaneamente file nei Data Vault.
- Una pianificazione per gli aggiornamento periodici, che verifica che tutti i file previsti per un utente siano presenti nel Data Vault e, in caso contrario, eventuali file mancanti vengono copiati. In questo modo si ha un'ulteriore garanzia che tutti i file degli utenti siano stati copiati correttamente nel Data Vault.
- Se fosse necessario eseguire un **aggiornamento iniziale** (o copia). L'aggiornamento iniziale è necessario perché durante il funzionamento normale Data Protector for PCs, ogni volta che un utente cambia un file con protezione di tipo continuo Data Protector for PCs, nel Data Vault vengono copiate solo le informazioni relative ai cambiamenti.

I criteri di copia predefiniti si applicano a tutti i Data Vault per i quali non sono stati definiti criteri di copia espliciti. È possibile cambiare le impostazioni per i criteri di copia, tuttavia non è possibile eliminarli o rinominarli.

Per creare un criterio di copia:

a. Fare clic su **Criteri** nel pannello di navigazione di sinistra.
b. Fare clic su **Imposta i criteri di copia**.
c. Fare clic su **Crea nuovo criterio di copia**.
d. Seguire le istruzioni nella finestra.

Buona prassi:

- **Limitazione**: impostare il periodo di tempo sull'orario normale di lavoro e impostare una limitazione inferiore per gli altri orari.
- **Aggiornamento iniziale**: abilitare l'aggiornamento iniziale per garantire che venga eseguito il backup di tutti i file degli utenti protetti dai criteri di protezione file.
- **Aggiorna file ogni settimana/mese**: se si tiene conto che un aggiornamento deve interessare poche copie di file, qualora ce ne fossero, abilitare gli aggiornamenti di Data Vault per garantire che sia effettuato il backup in modo accurato di tutti i file utente protetti da criteri.

4. **Configurazione dei criteri di protezione dei file.**

I criteri di protezione dei file consentono di specificare i file che devono essere protetti e per quanto tempo conservare le versioni precedenti. Ad esempio è possibile definire un criterio di protezione file denominato *Documenti di Office* per i documenti di Word, i fogli di calcolo Excel e le presentazioni PowerPoint.

I file salvati nelle unità disco locali possono essere protetti.

Esistono due tipi di criteri:

- **Continuous File Protection**—che fornisce la protezione in tempo reale dei file ogni volta che vengono salvati o cancellati dal disco. Generalmente, qualsiasi file o documento che consente di selezionare **Salva** dal menu dovrebbe essere protetto con un criterio Continuous File Protection.

  Data Protector for PCs comprende diversi esempi di criteri. Per impostazione predefinita, dopo l'installazione ne vengono selezionati tre: *Documenti Office*, *Sviluppo software* e *Documenti Web*. È possibile iniziare con questi criteri, oppure si possono creare criteri propri.

- **Open File Protection**—che fornisce la protezione dei file periodicamente (in genere una volta all'ora) scattando una istantanea del file. Generalmente, qualsiasi file molto grande (più di 100 MB), che rimane aperto per la maggior parte del giorno o che non ha l'opzione **Salva** nel menu, deve essere protetto con questo metodo. File comuni di questo tipo sono i file di posta elettronica e i database.

  Data Protector for PCs comprende quattro esempi: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* e *Thunderbird*. È possibile iniziare con questi criteri, oppure si possono creare criteri propri.

  NOTA: Data Protector for PCs non supporta il backup di file con crittografia EFS con criteri Open File Protection, pertanto i file .pst non devono avere crittografia EFS.

Per creare un criterio di protezione file:

a. Fare clic su **Criteri** nel pannello di navigazione di sinistra.

b. Fare clic su **Imposta i criteri di protezione file**.

c. Fare clic su **Crea nuovo criterio di Continuous File Protection** o **Crea nuovo criterio di Open File Protection**.

d. Seguire le istruzioni nella finestra.

NOTA: Quando si creano criteri File Protection e si impostano regole di esclusione o inclusione, le estensioni dei file non devono avere più di 9 caratteri per i criteri Open File Protection e di 29 caratteri per i criteri Continuous File Protection.

Per i criteri Open File Protection, è possibile selezionare file senza estensioni nelle regole di inclusione. Lo stesso non può essere fatto per i criteri Continuous File Protection.

IMPORTANTE: A questo punto si sono configurati tutti i criteri fondamentali necessari per Data Protector for PCs. Data Protector for PCs viene fornito già configurato con altri criteri che sono sufficienti per la maggior parte delle organizzazioni. Si raccomanda di iniziare a installare subito gli agenti su desktop e portatili (vedere "Installazione degli agenti Data Protector for PCs" (pagina 37)). Successivamente, è possibile riesaminare e configurare i criteri rimanenti per Data Protector for PCs, quali i criteri di Cleanup, criteri di controllo utenti, criteri di aggiornamento agente e i criteri di conservazione dati per reporting.

Configurazione dei criteri rimanenti

1. **Configurazione dell'accesso ad Active Directory**.

NOTA: *Associazione di gruppi Active Directory con Data Vault:* è possibile associare i Data Vault con i gruppi Active Directory nel criterio di Data Vault. Il backup di tutti i membri dei gruppi associati verrà eseguito sul Data Vault associato. I singoli utenti non possono essere associati. In seguito, se viene associata un'unità organizzativa (OU), verranno associati solo i gruppi nell'unità organizzativa. Ogni utente presente direttamente nell'unità organizzativa non viene associato con il Data Vault. L'elenco dei gruppi Active Directory può erroneamente includere gruppi diversi dai gruppi di sicurezza, ad esempio i gruppi di distribuzione. Tuttavia, solamente i gruppi di sicurezza saranno associati con un Data Vault.

Utenti multipli: se uno o più utenti stanno condividendo un computer, questi devono appartenere allo stesso gruppo Active Directory.

Se si desidera assegnare i Data Vault per gruppo o unità organizzative, o se si desidera creare report per gruppo o unità organizzativa, è necessario configurare Policy Server in modo che possa accedere al proprio Active Directory.

La configurazione dell'accesso ad Active Directory abilita l'opzione **Membri di gruppi e unità organizzative** per i Data Vaults (vedere "Prima configurazione" (pagina 24)).

Per configurare l'accesso ad Active Directory:

a. Fare clic su **Configurazione** nel pannello di navigazione di sinistra.

b. Fare clic su **Configura accesso ad Active Directory**.

c. Seguire le istruzioni nella finestra.

2. **Configurazione del criterio di Cleanup**.

   È necessario eseguire periodicamente il cleanup delle impostazioni dei Local Repository di Data Protector for PCs nei computer degli utenti e dei Data Vault nei server Data Vault per eliminare le versioni che sono precedenti rispetto alle impostazioni di conservazione definite nei criteri di protezione dei file.

   Per configurare il criterio di Cleanup:

   a. Fare clic su **Criteri** nel pannello di navigazione di sinistra.

   b. Fare clic su **Imposta i criteri di cleanup**.

   c. Seguire le istruzioni nella finestra.

   Per far sì che Data Vault supporti più utenti, eseguire il processo di Cleanup solo nei fine settimana, a partire dal venerdì sera o dal sabato mattina presto, in modo che possa essere eseguito con il massimo del tempo a disposizione:

   a. Aprire la pagina Criteri di Cleanup nella console di amministrazione del Policy Server e cambiare la **Pianificazione Cleanup del Data Vault**.

   b. Deselezionare tutti i giorni ad eccezione del venerdì o del sabato:

   - Per il venerdì, selezionare un orario di inizio nella tarda serata, ad esempio le 22.
   - Per il sabato, selezionare un orario di inizio al mattino presto, ad esempio le ore 1.

   Con il Cleanup in esecuzione solo nei fine settimana:

   - L'elenco dei file presentati per il ripristino da un Data Vault risulterà non essere aggiornato per un arco di tempo fino a una settimana. Gli utenti possono sempre eseguire l'analisi manuale dei dati sul Data Vault per ottenere una visualizzazione aggiornata.
   - Le versioni di backup vengono mantenute oltre la loro scadenza fino ad una settimana poiché il Cleanup viene eseguito solo nei fine settimana.
   - La gestione della quota non viene aggiornata. Se gli utenti superano la quota assegnata, devono attendere che venga eseguito il Cleanup per liberare spazio nel Data Vault. D'altro canto, il superamento della quota potrebbe non essere riconosciuto immediatamente dal sistema perché il report sull'utilizzo dello spazio è parte del processo di Cleanup.

   Buona prassi:

   - **Pianificazione Cleanup Local Repository**: Lasciare il valore predefinito di 1 ora.
   - **Pianificazione Cleanup del Data Vault**: L'impostazione predefinita "esegui il cleanup ogni giorno a mezzanotte" dovrebbe essere soddisfacente per la maggior parte delle installazioni. Fare riferimento a "Raccomandazioni sul dimensionamento" (pagina 32) per ulteriori informazioni sulla capacità del Data Vault.

- È possibile configurare DPNECleanup per utilizzare thread multipli in modo riutilizzabile ed estendibile per un utilizzo migliore di CPU e disco, consentendo l'archiviazione di più dati. Fare riferimento a "Configurazione di Cleanup multithread" (pagina 35).

3. **Configurazione dei criteri di controllo utenti**.

   I criteri di controllo utenti definiscono il livello di controllo degli utenti sui criteri corporate distribuiti sul computer.

   Per configurare i criteri di controllo utenti:

   a. Fare clic su **Criteri** nel pannello di navigazione di sinistra.
   b. Fare clic su **Imposta i criteri di controllo utenti**
   c. Seguire le istruzioni nella finestra.

   Buona prassi:

   Impostare **consenti controllo utenti** per **Recupero self-service**.

4. **Configurazione dei criteri di aggiornamento agente**.

   I criteri specificano la versione dell'agente Data Protector for PCs che deve essere utilizzata da tutti i desktop e computer portatili protetti da Data Protector for PCs che verranno aggiornati automaticamente a questa versione.

   Per configurare i criteri di aggiornamento agente:

   a. Fare clic su **Criteri** nel pannello di navigazione di sinistra.
   b. Fare clic su **Imposta i criteri di aggiornamento agente**.
   c. Seguire le istruzioni nella finestra.

5. **Configurazione della conservazione dei dati per il reporting**.

   Imposta il periodo di tempo per il quale i dati vengono conservati per i report per ognuna della categorie principali di informazioni.

   Per configurare la conservazione dei dati per il reporting:

   a. Fare clic su **Configurazione** nel pannello di navigazione di sinistra.
   b. Fare clic su **Configura conservazione dati per reporting**
   c. Seguire le istruzioni nella finestra.

Altre attività di configurazione

In genere vengono eseguite quando si installata Data Protector for PCs per la prima volta.

Ottenere la licenza per il software Data Protector for PCs.

Se si sta valutando Data Protector for PCs, può essere usato per 60 giorni per proteggere un numero di utenti illimitato senza che sia necessario avere un'ulteriore licenza. Quando si acquista Data Protector for PCs, è necessario visitare HP License Key Delivery Service

all'indirizzo https://webware.hp.com/welcome.asp per scaricare il codice di licenza che è possibile utilizzare.

Per immettere un codice di licenza:

1. Fare clic su **Gestione licenze** nel pannello di navigazione di sinistra.
2. Fare clic su **Immettere un codice di licenza per HP Data Protector for PCsutenti**.
3. Seguire le istruzioni nella finestra.

Se si devono immettere più licenze, è possibile creare un file di testo con una stringa con il codice di licenza per ogni riga. Il file può essere importato usando il campo Importa codice di licenza.

NOTA: Le licenze vengono distribuite agli agenti quando vengono installati.

Come spostare le licenze

Se è necessario cambiare l'indirizzo IP del Policy Server per spostare il server su un altro sistema, o se si devono spostare le licenze da un Policy Server a un altro, contattare HP License Key Delivery Service su https://webware.hp.com/welcome.asp.

Impostare, importare e esportare una password di crittografia.

Per garantire la protezione, è necessario definire una password di crittografia prima di poter utilizzare Data Protector for PCs. In questo modo si garantisce che tutti i file sono crittografati nel computer dell'utente e che vengono crittografati qaundo sono trasmessi in rete. La stessa password viene usata per crittografare i file da tutti gli utenti e per tutti i Data Vault configurati a livello centrale.

- Un Data Vault definito a livello centrale (definito tramite la console di Policy Server) usa sempre la crittografia in relazione alla password di crittografia per Data Protector for PCs.
- Con i Data Vault definiti a livello centrale (definiti dagli utenti utilizzando i propri computer), gli utenti possono scegliere se utilizzare la crittografia o meno e scegliere le password desiderate.

Quando si installa Data Protector for PCs per la prima volta, prima di poter proseguire è necessario generare o importare una password. Dopo avere generato una password, per la propria sicurezza, esportare la password. In questo modo viene salvata in una posizione protetta. Può essere importata successivamente.

NOTA: Non è possibile cambiare password dopo averla generata o importata.

Per gestire la propria password di crittografia:

1. Fare clic su **Criteri** nel pannello di navigazione di sinistra.
2. Fare clic su **Criteri di crittografia**.
3. Seguire le istruzioni nella finestra.

Determinazione del numero di Agenti che possono essere supportati

È molto difficile fornire delle regole generali valide in tutti gli ambienti, pertanto, i casi illustrati di seguito descrivono in modo chiaro il contesto per il quale i numeri specificati sono validi.

Fattori che influiscono sul dimensionamento

Il dimensionamento di un ambiente Data Protector for PCs è complesso. I fattori tecnici che influiscono sul numero di utenti supportati da un ambiente specifico includono:

- Potenza del processore sul Data Vault (per il consolidamento notturno dei dati di backup)
- Rete e larghezza di banda per I/O sul server Data Vault
- Spazio su disco sul server Data Vault
- Dimensione del database SQL sul Policy Server
- Larghezza di banda della rete e potenza del processore sul Policy Server

Quali di queste possa generare un collo di bottiglia in una qualsiasi installazione specificata è determinato sia dalle impostazioni di configurazione di Data Protector for PCs che dai criteri di utilizzo:

- Numero di utenti su un Data Vault
- Numero e dimensione dei file coperti dai criteri di protezione configurati
- Frequenza delle modifiche dei file protetti
- Impostazioni di conservazione per i tipi di file protetti

Raccomandazioni sul dimensionamento

Data Vault

Con una pianificazione giornaliera del Cleanup, un Data Vault con 14TB di spazio sul disco può supportare una popolazione fino a **3.500** Agent se le caratteristiche medie dei dati sono circa:

- Numero medio di file protetti: 5000
- Dimensione totale media dei file protetti sul disco locale: 10 GB
- Dimensione totale media sul Data Vault (compresso): 4 GB

Se è necessario proteggere una quantità di dati che è mediamente superiore a quanto indicato in questo esempio, è sufficiente aumentare la capacità del disco nel Data Vault per creare più spazio per i dati, anche se il Data Vault non sarà in grado di completare

il consolidamento notturno dei dati di backup nel tempo previsto. Considerare le seguenti possibilità:

- Eseguire il cleanup del Data Vault solo nei fine settimana. Fare riferimento al passaggio 2 "Configurazione del criterio di Cleanu" in “Configurazione dei criteri rimanenti” (pagina 28) per informazioni su come procedere. In questo modo si dovrebbe incrementare a 10.000 il numero di agenti che possono essere supportati da un Data Vault con 40TB di spazio sul disco, specificando le stesse caratteristiche medie dei dati.
- Prendere in esame la possibilità di distribuire i dati dell'utente finale su diversi Data Vault.

Le specifiche hardware per questi Data Vault sono:

Tipo di Data Vault	Cleanup giornaliero (fino a 3.500 agenti)	Cleanup settimanale (fino a 10.000 agenti)
Condivisione di file Windows	3 GHz dual core, 4 GB RAM, 14 TB di spazio sul disco	3 GHz dual core, 4 GB RAM, 40 TB di spazio sul disco
Data Vault Web	3 GHz quad core, 4 GB RAM, 14 TB di spazio sul disco	3 GHz quad core, 4 GB RAM, 40 TB di spazio sul disco

Se gli utenti dispongono mediamente di una quantità minore di dati, potrebbe essere possibile ospitare un numero maggiore di utenti su un Data Vault.

NOTA: HP raccomanda vivamente di conservare il sistema operativo del Data Vault e i dati di backup su dischi fisici separati per avere prestazioni ottimali.

Per prestazioni ottimali il disco del Data Vault deve essere deframmentato regolarmente.

Policy Server

La quantità di traffico generato sul Policy Server dipende direttamente dal numero di Agenti ospitati sul server. L'uso dell'edizione Express di MS SQL Server inclusa con Data Protector for PCs impone una dimensione massima del database di 4 GB e non più di 5.000 agenti[1] sono supportati.

Nel caso sia necessario supportare più di 5.000 Agent nell'ambiente, è possibile disporre di ulteriori Policy Server o sostituire MS SQL Express con la versione completa di Microsoft SQL Server. In questo modo, il Policy Server può essere aumentato fino a 50.000 Agent. Se si decide di utilizzare la versione completa di MS SQL Server, prendere in considerazione la necessità di aggiornare la memoria principale di Policy Server, portandola ad almeno 3GB.

1. Utilizzo dell'impostazione predefinita "conservazione dei dati per il reporting" sul Policy Server per 30 giorni.

Per le prestazioni, il Policy Server deve essere eseguito su un server diverso dal server Data Vault. È possibile fare in modo che siano in esecuzione sullo stesso server, ma questa disposizione viene consigliata solo per valutare il prodotto.

Deve essere presente almeno un Policy Server anche se non è necessario avere un numero corrispondente di Data Vault e Policy Server.

Considerazioni sulla rete

NOTA: I Data Vault Web non sono interessati da latenza elevata. Le informazioni riportate di seguito si riferiscono solo ai Data Vault sulle condivisioni di file Windows.

In generale sui Data Vault sulle condivisione di file Windows, HP non raccomanda di eseguire un aggiornamento iniziale dai Agent di Data Protector for PCs a Data Vault se la latenza della rete tra i due è superiore a 50 ms. Ciò in genere si applica agli uffici domestici o agli uffici remoti con una connessione WAN lenta. L'aggiornamento iniziale funziona ma richiederà più tempo.

Se l'ambiente include uffici in diversi siti e la latenza di rete per questi è inferiore a 50 ms, considerare l'installazione di Data Vault si più di un sito in modo che tutti gli uffici possano raggiungere almeno un Data Vault con una latenza di 50 ms o inferiore.

Una volta completato l'aggiornamento iniziale, gli aggiornamenti possono essere eseguiti da una qualsiasi posizione all'interno della rete aziendale o dall'ufficio domestico. In genere questi sono sufficientemente piccoli da funzionare anche in caso di connessioni di rete lente.

Se l'aggiornamento iniziale viene eseguito tramite una connessione con latenza elevata, potrebbe richiedere diversi giorni per il completamento, e può essere interrotto senza errori. Data Protector for PCs continuerà l'aggiornamento dal punto in cui è stato interrotto non appena viene riconnesso al Data Vault.

SUGGERIMENTO: Se non si conosce la latenza tra gli uffici, utilizzare il comando `ping` da un computer in un sito per inviare un ping a un computer in un altro sito. Ciascun ping con esito positivo riporterà la latenza.

5 Configurazione di Cleanup multithread

Le prestazioni di `DPNECleanup` limitano la quantità di dati degli utente per il backup su un Data Vault. È possibile configurare DPNE Cleanup per utilizzare thread multipli in modo riutilizzabile ed estendibile per un utilizzo migliore di CPU e disco, consentendo l'archiviazione di più dati.

Con il Cleanup multithreaded, l'argomento del Pianificatore `-s` porta agli argomenti predefiniti `-e -f -u -p -d 1000`, compreso il Cleanup multithreaded predefinito e a un ritardo di 1 secondo per il Regolatore automatico. Se non si desidera utilizzare questi valori predefiniti, ad esempio, per disabilitare l'esecuzione multithread, eliminare l'argomento '-s' dalla chiamata del Pianificatore e aggiungere i singoli argomenti CLI.

NOTA:

Sebbene in alcune circostanze si potrebbe voler disabilitare il Cleanup multithreaded, si raccomanda di conservare `-e -f -u` come argomenti per la chiamata di Cleanup sul Data Vault.

Utilizzo di DPNECleanup.exe da CLI

L'argomento `-p` a `DPNECleanup.exe` consente al Cleanup di inizializzare e avviare il motore parallelo e pertanto di abilitare l'esecuzione multithreaded. Il motore parallelo mette a disposizione sette argomenti opzionali per le righe di comando L'eseguibile DPNECleanup è in grado di recuperare questi argomenti e li trasferisce al motore parallelo.

DPNE Cleanup viene eseguito in modalità seriale se non si imposta `-p`. In questa modalità il motore parallelo non viene usato.

dpnecleanup

`-a` *`affinity`*
Imposta l'affinità del processore sul numero specificato, che riflette i bit impostati per i core della CPU utilizzati dai thread.

`d` *`delay`*Imposta il ritardo in millisecondi prima dell'intervento dell'Auto regolatore, lascia al motore parallelo il tempo per avviare una serie di thread e creare un utilizzo del sistema. Per impostazione predefinita l'argomento `-s` crea un ritardo di 1000 millisecondi, o di 1 secondo.

`-m` *`maxCpuUsage`*
Imposta l'utilizzo massimo desiderato della CPU (per tutti i core definiti da `affinity`) in *`maxCpuUsage`*%, che l'Auto regolatore proverà a raggiungere. *`maxCpuUsage`* deve essere un valore intero compreso tra 1 e 100. L'impostazione predefinita è '0' che equivale a nessun limite (uso totale della CPU).

`-o`

Risorse costanti, indica che l'Auto regolatore è disabilitato e pertanto il motore parallelo non cambierà il numero di thread simultanei. Usare `-r` per specificare il numero di thread simultanei. Gli argomenti `-d`, `-m` e `-q` sono ignorati quando sono in esecuzione con `-o`.

`-p`
Abilita il Cleanup multithread.

`-q` *`maxQueueLength`*
Imposta la lunghezza media massima desiderata della coda del disco a cui l'Auto regolatore cercherà di adeguarsi. Il valore è un numero mobile. Il valore predefinito è 2,0.

`-r` *`resourceCount`*
Imposta il numero di risorse simultanee (thread) in relazione al numero specificato. Per impostazione predefinita e in combinazione con l'opzione `-o`, il sistema opererà con 2^(numero di CPU) thread simultanei. Se l'Auto regolatore è in esecuzione, il valore specificato rappresenta il limite di risorse simultanee in termini di thread. Il numero massimo predefinito è 0, che indica nessun limite.

`z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`
Imposta la priorità del processo per tutti i thread. Il valore predefinito è `Normal`.

`-s`
Cleanup del server. Imposta il Cleanup per tutti i Data Vault, sia quelli definiti a livello centrale, che quelli definiti dall'utente. Con il comportamento multithreaded, viene sostituito dagli argomenti '`-e -f -u -p -d 1000`' quando si esegue il comando.

`-e`
Cleanup a livello aziendale. Imposta il Cleanup per tutti i Data Vault che sono definiti a livello centrale dai criteri dal Policy Server.

`-f`
Cleanup rapido. Di norma il Cleanup agenti viene eseguito solo se il sistema è inattivo. Questa opzione consente di avviare il Cleanup in qualsiasi momento.

`-u`
Cleanup definito dall'utente. Imposta il Cleanup per tutti i Data Vault locali che sono definiti da criteri locali creati dall'utente.

6 Installazione degli agenti Data Protector for PCs

NOTA: Le licenze vengono distribuite agli agenti quando vengono installati.

Gli agenti Data Protector for PCs possono essere installati in due modi:

- Singolarmente su ogni computer client. Vedere "Installazione degli agenti Data Protector for PCs su singoli computer client" (pagina 37).
- Distribuiti nell'organizzazione da un file server accessibile a tutti i computer client. Vedere "Distribuzione di Data Protector for PCs Agent nell'organizzazione" (pagina 38).

Installazione degli agenti Data Protector for PCs su singoli computer client

Prerequisiti

Il software agente di Data Protector for PCs può essere installato nei desktop e nei portatili degli utenti con Windows. Per le piattaforme supportate, fare riferimento alla matrice del supporto.

È necessario eseguire l'accesso all'account con i privilegi amministratore.

Procedura di installazione

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Viene avviata subito la procedura di installazione. In caso contrario, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione.
2. Fare clic su **Installa o aggiorna software agente Data Protector for PCs**. Scegliere **Apri** (o **Esegui**) se viene visualizzata la finestra di dialogo "Apri o Salva".
3. Se il computer dell'utente non ha Microsoft Windows Installer 3.1 o successivo installato, la procedura guidata consente di installarlo. Quando viene visualizzata la finestra di dialogo Aggiornamento di Windows Installer, fare clic su **OK** per installarlo.
4. Se il computer dell'utente non ha Microsoft .NET Framework 2.0 SP1 o successivo installato, la procedura guidata consente di installarlo. Quando viene visualizzata la finestra di dialogo Aggiornamento di .NET Framework 2.0 SP1, fare clic su **OK** per installarlo.
5. La procedura guidata installa automaticamente l'agente di Data Protector for PCs. Seguire le istruzioni riportate sullo schermo. Durante l'installazione, verrà chiesto di inserire i dettagli del Policy Server.

6. Una volta completata l'installazione e la configurazione, fare clic su **Fine**. Se su Policy Server è impostato un criterio di Open File Protection, verrà chiesto di riavviare il sistema.

   A questo punto nella barra delle applicazioni viene visualizzata l'icona Data Protector for PCs (in relazione allo stato della protezione viene visualizzata una di queste icone: ).

7. Eseguire il test per verificare che l'agente di Data Protector for PCs funzioni correttamente:
   a. Selezionare o creare un file di test, ad esempio un documento Word o un foglio di lavoro Excel, ad esempio sul desktop. Eseguire delle modifiche nel documento e fare clic su **Salva**.
   b. Fare clic con il tasto destro sul file di test dal desktop, da Esplora risorse o nella finestra di dialogo Apri. Nel menu visualizzato devono essere presenti tre voci di Data Protector for PCs (**Cerca e recupera file...**, **Copia versione** e **Apri versione con *XXX*...**).
   c. Selezionare **Apri versione con *XXX*...** per visualizzare un elenco di tutte le versioni con l'indicazione di data e ora del documento appena creato o modificato. Selezionando una delle versioni, questa viene aperta come documento in sola lettura utilizzando l'applicazione appropriata. In questo modo l'utente è in grado di recuperare le versioni precedenti dei documenti dal local repository di Data Protector for PCs.
8. Ripetere i passaggi da 1 a 8 per gli altri desktop e computer portatili che si desidera proteggere utilizzando Data Protector for PCs.

Distribuzione di Data Protector for PCs Agent nell'organizzazione

Inizialmente gli Agenti di Data Protector for PCs possono essere deistribuiti nell'organizzazione utilizzando il kit di distribuzione Data Protector for PCs Agent contenuto nel CD-ROM di installazione.

NOTA: Il kit di distribuzione non può essere utilizzato su computer Vista con UAC (User Account Control) abilitato. Per correggere il problema, disabilitare UAC o installare interattivamente l'agente.

Nella procedura descritta di seguito, per prima cosa copiare il kit di distribuzione di Data Protector for PCs Agent in *CD-ROM*:\Agent nella directory su un file server accessibile a tutti gli utenti. Quindi creare un file dei parametri all'interno della directory utilizzando `SetupConfig.exe`. In conclusione, stabilire un meccanismo per eseguire `StartInstall.exe` nella directory condivisa da ciascun computer degli utenti. Ad esempio, è possibile utilizzare uno script di login. È quindi possibile monitorare la distribuzione utilizzando il report distribuzione Agenti dalla console di Policy Server di Data Protector for PCs.

Contenuti del kit

Il kit di distribuzione di Data Protector for PCs contiene i seguenti componenti:

`SetupConfig.exe`	Crea e modifica il file di inizializzazione.
`StartInstall.exe`	Avvia `Setup.exe` come utente privilegiato.
`Setup.exe`	Installa i prerequisiti e `DataProtectorNE.ini`.
`DataProtectorNE.msi`	Pacchetto Windows Installer di Data Protector for PCs per installare il software dell'agente.
`DataProtectorNE64.msi`	Pacchetto Windows Installer di Data Protector for PCs per installare il software dell'agente su computer a 64–bit.
`DataProtectorNE*.*.mst`	Pacchetti Windows Installer di Data Protector for PCs per installare il software dell'agente localizzato.
`WindowsInstaller.exe`	Aggiorna Windows Installer (necessario per l'installazione .NET).
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	Installa NET Framework 2.0 SP1.
`Setup.ini`	File dei parametri per la configurazione dell'installazione di Data Protector for PCs. Questo file viene creato utilizzando `SetupConfig.exe` (fare riferimento al passaggio 4 di seguito).

Procedura di distribuzione e installazione

1. Copiare i file nella directory Agente del CD-ROM di distribuzione nella directory accessibile da tutti gli utenti che intendono utilizzare il kit di distribuzione Data Protector for PCs Agent. Può essere la directory di una condivisione netlogon comune, ad esempio `\\yourserver\DPNEDeploy`.
2. Assicurarsi che la nuova directory contenga i file elencati in precedenza. Tutti gli altri file possono essere eliminati.
3. Aprire una finestra di comandi DOS (`cmd.exe`) e `cd` alla directory creata nel passaggio 1.
4. Eseguire `SetupConfig.exe` per creare o modificare il file dei parametri `Setup.ini`. La prima volta che si esegue `SetupConfig.exe`, è necessario specificare i valori per tutti i parametri. Una volta completato, è possibile eseguire più volte `SetupConfig.exe` per cambiare i parametri. Per non cambiare un parametro, è sufficiente premere **Invio**.

   I parametri richiesti sono:

   - **Il percorso UNC ai pacchetti di installazione** – il percorso completo per la directory condivisa nella quale vengono copiati i file nel passaggio 1, ad esempio `\\yourserver\DPNEDeploy`.

- Il nome di **Data Protector for PCs Policy Server**. Può essere un nome NetBIOS, ad esempio `YOURSERVER`, o un nome dominio completo, ad esempio `yourserver.yourcompany.com`.
- **Nome utente** – il nome utente di un utente con privilegi di amministratore sui computer che utilizzano il kit di distribuzione di Agent diData Protector for PCs, ad esempio un membro del gruppo Amministratori di dominio. In genere è un nome utente completo che include il dominio, ad esempio `YOURCOMPANY\JerryAdmin`.
- **Password** – la password associata con il nome utente. Digitare la password due volte per confermarla.

5. Sul computer client, eseguire `StartInstall.exe`, ad esempio `\\yourserver\DPNEDeploy\StartInstall`. `Setup.exe` verrà quindi eseguito in background con una prioprità di livello basso utilizzando il nome utente e la password specificati in `Setup.ini`. Può essere eseguito come parte di uno script di login. Non è possibile includerlo nello script di avvio perché l'account del computer non dispone di privilegi di rete sufficienti.
6. `Setup.exe` determina se il computer client può supportare Data Protector for PCs. Per le piattaforme Windows supportate, fare riferimento alla matrice del supporto.
7. `Setup.exe` determina se è intallata la versione 2.0 SP1 di .NET Framework. In caso contrario, verrà installata; al termine dell'installazione sarà necessario riavviare il computer.
8. `Setup.exe` determina se Data Protector for PCs è già installato. In caso contrario o se la versione non è aggiornata, Data Protector for PCs viene installato.

NOTA:

In caso di errori nei passaggi 4–7 verrà registrato un messaggio su Policy Server di Data Protector for PCs e nel Registro evento dell'applicazione sul computer locale.

È possibile verificare l'avanzamento della distribuzione dell'Agente utilizzando la console di Data Protector for PCs Policy Server:

1. Accedere alla console di Data Protector for PCs Policy Server.
2. Selezionare **Distribuzione Agent** in **Report** nel pannello di navigazione di sinistra.

   Viene visualizzato un riepilogo della distribuzione iniziale per data. Mostra:

   - Il numero di computer che hanno **terminato** con successo la distribuzione.
   - Il numero dei computer per i quali la distribuzione è **in corso**.
   - Il numero di computer per i quali la distribuzione **non è riuscita**.

3. Fare clic su un numero nella colonna **Numero di computer** per visualizzare l'elenco dei computer nello stato di distribuzione selezionato.

   Viene visualizzato lo stato corrente di ogni computer. Ad esempio, se la distribuzione di un computer specifico non è riuscita, la colonna **Informazioni** indica l'errore che si è verificato. È possibile ottenere altre informazioni relative al computer facendo clic sul relativo nome NETBIOS.

7 Aggiornamento di Data Protector for PCs

Se si sta eseguendo l'aggiornamento della versione 6.*x* di Data Protector for PCs all 7.0, procedere nell'ordine seguente:

1. Aggiornamento di Policy Server a 7.0 Fare riferimento a "Aggiornamento del Policy Server" (pagina 42).
2. Installare il software per il server Data Vault Web. Fare riferimento all'installazione di un web "Installazione, configurazione e manutenzione del server Data Vault Web." (pagina 18).
3. Aggiornare gli agenti alla 7.0.

   È possibile aggiornarli utilizzando Aggiornamento manuale o "automaticamente" utilizzando i Criteri di aggiornamento agente. Fare riferimento a "Aggiornamento degli agenti" (pagina 42) per maggiori informazioni.

Aggiornamento del Policy Server

È possibile aggiornare un'installazione esistente di Data Protector for PCs Policy Server a una versione e più recente seguendo la procedura standard per l'installazione. Tutte le configurazione esistenti (ad esempio la configurazione Data Vault, Gestione licenze, e così via) saranno disponibili nella nuova versione.

Aggiornamento del Policy Server

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Se la procedura guidata di installazione non viene avviata automaticamente, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione.
2. Fare clic su **Installa Policy Server** nella pagina Installa Data Protector for PCs della procedura guidata per iniziare l'aggiornamento.
3. Seguire le istruzioni riportate sullo schermo.
4. La procedura di installazione rileverà l'installazione di Policy Server esistente e consentirà di eseguire un aggiornamento.
5. Seguire le istruzioni riportate sullo schermo.
6. Una volta completata l'installazione, fare clic su **Avanti** . A questo punto è possibile eseguire la console Data Protector for PCs Policy Server.

NOTA: Se il software Cleanup è installato in Policy Server, è necessario aggiornarlo. È possibile eseguire l'aggiornamento manualmente o tramite i Criteri di aggiornamento agente.

Aggiornamento degli agenti

Se la versione del server Data Protector for PCs viene aggiornata, gli agenti che utilizzano la versione precedente di Data Protector for PCs continueranno a funzionare come prima.

È possibile aggiornarli utilizzando Aggiornamento manuale o "automaticamente" utilizzando i Criteri di aggiornamento agente.

NOTA: Dopo l'aggiornamento è necessario riavviare tutti gli agenti in modo che possano utilizzare i nuovi Data Vault Web. L'istruzione viene presentata dall'area commenti nella barra delle applicazioni e anche nella scheda Riepilogo del riquadro Integrità di Data Protector for PCs sui rispettivi PC.

Aggiornamento automatico dell'agente utilizzando i criteri di aggiornamento dell'agente

Gli agenti possono essere "aggiornati" automaticamente utilizzando i Criteri di aggiornamento dell'agente del Policy Server. Il pacchetto di installazione verrà inviato automaticamente a tutti i client connessi e l'aggiornamento verrà completato automaticamente. Le operazione dell'utente finale non vengono interrotte.

1. Nella console di Policy Server, selezionare **Criteri->Criteri di aggiornamento agente**.
2. Se Policy Server è stato appena aggiornato, è stato caricato anche un nuovo Pacchetto di aggiornamento agente dalla procedura di installazione. Nella console di Policy Server, questa nuova versione non è ancora stata selezionata.

   Selezionare la nuova versione dell'agente per rendere la versione disponibile.
3. Agendo sulla Limitazione, è possibile regolare il numero massimo di aggiornamenti consentiti al minuto.
4. Fare clic su **Salva criteri di aggiornamento agente**.
5. I nuovi agenti saranno aggiornati automaticamente alla versione più recente. Verranno aggiornati automaticamente anche gli agenti Cleanup.

NOTA: È possibile controllare l'avanzamento dell'aggiornamento dell'agente utilizzando il report: "Distribuzione agente".

Aggiornamento manuale dell'agente

È possibile aggiornare un agente di Data Protector for PCs esistente alla versione più recente eseguendo la procedura di installazione standard.

Prima di aggiornare l'agente alla versione più recente, assicurarsi che la versione dell'agente sia conforme alla versione di Data Protector for PCs Policy Server.

1. Inserire il CD-ROM di installazione di Data Protector for PCs. Se la procedura guidata di installazione non viene avviata automaticamente, avviarla manualmente facendo doppio clic su `setup.hta` nella radice del CD-ROM di installazione
2. Fare clic su **Installa agente** nella pagina Installa Data Protector for PCs della procedura guidata per iniziare l'aggiornamento.
3. Seguire le istruzioni riportate sullo schermo.
4. La procedura di installazione rileverà l'installazione esistente dell'agente e consentirà di eseguire un aggiornamento.
5. Seguire le istruzioni riportate sullo schermo.

8 Come ricevere assistenza per Data Protector for PCs

Data Protector for PCs viene fornito con un anno di manutenzione. Da diritto a:

- Supporto telefonico per parlare con un tecnico del Supporto.
- aggiornamenti del server Data Protector for PCs e del software Agent di Data Protector for PCs . È possibile scaricare le versioni più recenti o l'immagine del CD-ROM dal sito web Data Protector. Visitare http://www.hp.com/go/dataprotector.

Glossario

Active Directory
(Termine specifico di Windows) Il servizio directory in una rete Windows. Contiene informazioni sulle risorse disponibili nella rete e le rende disponibili per gli utenti e per le applicazioni. I servizi directory mettono a disposizione un modo coerente per assegnare il nome, descrivere, individuare, accedere e gestire risorse a prescindere dal sistema fisico su cui sono residenti.

Agent
Data Protector for PCs software in esecuzione sui desktop/computer portatili degli utenti. Le comunicazioni con Policy Server avvengono utilizzando i servizi Web (SOAP e XML) su TCP porta 80.

aggiornamento iniziale
Data Protector for PCs protegge continuamente i file ogni volta che gli utenti li cambiano salvando le modifiche. Tutte le volte che un utente crea un nuovo Data Vault, Data Protector for PCs deve creare un aggiornamento iniziale di tutti i file protetti dell'utente sul vault. Gli utenti possono scegliere come eseguire l'aggiornamento iniziale, immediatamente o in background.

console
La console basata sul browser viene usata per definire a livello centrale i criteri di Data Protector for PCs. È necessario far parte del gruppo Amministratori.

Continuous File Protection
Continuous File Protection è il metodo Continuous Data Protection di Data Protector for PCs, che archivia automaticamente i cambiamenti in un file a ogni salvataggio del file. È idoneo per file dati che sono salvati dall'utente (rispetto ai file di tipo sempre aperto quali i database o i file di Outlook). Ogni criterio Continuous File Protection protegge un gruppo di file che hanno una correlazione. Data Protector for PCs viene fornito con criteri già configurati per tipi di file usati più comunemente, quali i documenti di Office e le immagini. I criteri per la protezione dei file possono essere modificati, oppure è possibile creare altri criteri. Il criterio specifica anche il periodo di tempo per il quale vengono conservati i file protetti.

Criteri di Cleanup
I periodi di conservazione definiti dai criteri per la protezione dei file sono applicati dalle attività di Cleanup che vengono eseguite periodicamente. La frequenza viene definita nei criteri di Cleanup. Per impostazione predefinita, il cleanup dei Local Repository degli utenti viene eseguito ogni ora, e il cleanup dei Data Vaults definiti a livello locale viene eseguito una volta al giorno. Sui Data Vault definiti a livello centrale sulle condivisioni di file Windows il Cleanup viene eseguito da un computer assegnato dal criterio di Data Vault, e per i Data Vault Web il Cleanup viene eseguito a livello locale sul server Data Vault. I criteri di Cleanup si applicano a tutti gli utenti.

Criteri di controllo utenti
Questi criteri stabiliscono in che misura i singoli utenti possono controllare il Agentsoftware in esecuzione sui loro desktop/portatili/notebook. È possibile bloccare l'Agente in modo da nascondere i criteri agli utenti, ovvero gli utenti possono visualizzare i criteri, ma non possono modificarli, oppure si può consentire agli utenti di aggiungere i propri criteri. Il livello di controllo per ogni criterio Data Protector for PCs principale può essere definito separatamente. I criteri di controllo utenti si applicano a tutti gli utenti.

Criteri di copia
I criteri di copia definiscono i seguenti elementi:

- Il numero di Agenti che può copiare file contemporaneamente nei Data Vault.
- Una pianificazione per gli aggiornamento periodici, che verifica che tutti i file previsti per un utente siano presenti nel Data Vault e, in caso contrario, eventuali file mancanti vengono copiati. In questo modo si ha un'ulteriore garanzia che tutti i file degli utenti siano stati copiati correttamente nel Data Vault.
- Se fosse necessario eseguire un *aggiornamento iniziale*. L'aggiornamento iniziale è necessario perché durante il funzionamento normale di Data Protector for PCs, ogni volta che un utente cambia un file con protezione di tipo continuo Data Protector for PCs, nel Data Vault vengono copiate solo le informazioni relative ai cambiamenti.

Se Data Protector for PCs è stato appena installato, è necessario definire un criterio di copia per poter eseguire l'aggiornamento iniziale di tutti i file protetti dell'utente.

criterio Un criterio è una serie di regole, definite a livello centrale in Policy Server ed eseguite da Agent su ogni desktop/portatile/notebook.

Data Vault Esistono due tipi di Data Vault:

- Data Vault Web. Utilizzano il protocollo HTTPS e forniscono il livello migliore di protezione per la trasmissione dei dati tra i PC client e il Data Vault, offrono la migliore velocità effettiva in ambienti a elevata latenza, e pertanto sono raccomandati.
- Data Vault sulle condivisioni di file Windows Si tratta di cartelle condivise su un file server in cui vengono archiviati i file in base al criterio Data Vault. Il file server deve supportare il protocollo di condivisione file di Windows (CIFS/SMB). Non devono essere utilizzati in ambienti con latenza elevata della rete.

I dati hanno la medesima struttura su entrambi i tipi di Data Vault, pertanto è possibile convertire Data Vault sulle condivisioni di file Windows in Data Vault Web.

Uno o più criteri di Data Vault possono essere assegnati agli utenti in relazione al loro gruppo o all'appartenenza a un'unità dell'organizzazione.

file protetti Un file protetto è un file il cui backup viene eseguito automaticamente da Data Protector for PCs. I tipi di file protetti sono definiti nei criteri Continuous e Open File Protection.

Local Repository Local Repository è una posizione per l'archiviazione sicura sui computer Agent. Viene utilizzato per archiviare file protetti e i cambiamenti dei file, di solito su un disco rigido di sistema. Si tratta di una directory di sistema nascosta. Gli utenti possono recuperare rapidamente una versione precedente facendo clic con il tasto destro sul desktop, in Esplora risorse o in una finestra di dialogo aperta. I file protetti dai criteri Continuous File Protection vengono conservati in una directory nascosta nel computer locale fino al termine del periodo di conservazione. I file protetti dai criteri Open File Protection vengono archiviati temporaneamente nel Version Store locale fino a quando non sono copiati nel Data Vault. Il percorso del Local Repository è di solito `C:\{DPNE}`.

Open File Protection Open File Protection esegue il backup dei file che sono sempre aperti, quali ad esempio le cartelle personali di Outlook e i file di molti database grazie alla cattura regolare di un'istantanea a livello di file. Questa procedura viene anche definita "quasi" Continuous Data Protection. In criterio di Open File Protection definisce la protezione per i file aperti, che viene determinata da serie di regole per l'inclusione e l'esclusione. Ad esempio, è possibile definire un criterio denominato "Cartelle personali di Outlook" applicabile ai file .pst di Outlook, specificando una regola di inclusione del tipo "termina con '.pst'. Per escludere i file .pst archiviati, è possibile creare una regola di esclusione del tipo "contiene 'archivio'". I criteri specificano anche il periodo di tempo per il quale vengono conservati i file protetti. I criteri Open File Protection si applicano a tutti gli utenti.

Policy Server Policy Server consente di gestire in modo centralizzato i criteri di Data Protector for PCs. Raccoglie inoltre informazioni di stato da Agent e mette a disposizione report su distribuzione e funzionamento.

Utente con privilegi amministrativi

Utente di un server Data Vault sul web che ha compiti che richiedono privilegi amministrativi quali la creazione e la cancellazione di Data Vault e la migrazione dei dati di backup dei client.

Utente per il backup Utente di un server Data Vault Web che esegue operazioni tipiche dell'utente finale quali il backup e il ripristino di file.

Indice

E

F

G

H

I

L

M

N

P

R

S

U

V

W