HP Data Protector for PCs 7.0
Guía de instalación y administración

N° de referencia de HP: n. c.
Publicado: Junio de 2011
Edición: Primera

Contenido

Acerca de esta guía....5
Público objetivo....5
Convenciones y símbolos empleados en este documento....5
Información general....6
HP, soporte técnico....6
Servicio de suscripción....6
Sitios web de HP....7
Comentarios acerca de la documentación....7
1 Aspectos generales y requisitos previos....8
Aspectos generales de Data Protector for PCs....8
Data Vaults....9
Gestión de certificados....10
Certificados autofirmados....10
Certificados importados....10
Intercambio del certificado....11
Aspectos generales de la instalación de Data Protector for PCs....11
Requisitos previos....12
Policy Server....12
Base de datos....13
Data Protector for PCs Servidor web de Data Vaults....13
Agentes de Data Protector for PCs....13
2 Instalación de Policy Server de Data Protector for PCs....14
Instalación rápida....14
Instalación detallada....15
3 Instalación, configuración y mantenimiento del servidor web de Data Vaults....18
Instalación y configuración del servidor web de Data Vaults....18
Mantenimiento de los Data Vaults web....19
Migración de datos de un Data Vault basado en un recurso compartido de archivos de Windows a un Data Vault web....20
Configuración de las opciones de un Data Vault web desde la interfaz CLI (DvConfig)....21
4 Configuración de las políticas de protección de Data Protector for PCs....23
Configuración inicial tras la instalación de Data Protector for PCs....23
Configuración por primera vez....24
Configuración de las políticas restantes....28
Otras tareas de configuración....31
Determinación de cuántos Agents se pueden admitir....32
Factores que afectan al tamaño....32
Recomendaciones de tamaño....32
Data Vault....32
Policy Server....33

Consideraciones de redes....34
5 Configuración del proceso Cleanup con subprocesos....35
Uso de DPNECleanup.exe para la interfaz CLI....35
6 Instalación de agentes de Data Protector for PCs....37
Instalación de los agentes de Data Protector for PCs en equipos cliente individuales....37
Requisitos previos....37
Procedimiento de instalación....37
Implementación de Agents de Data Protector for PCs en una empresa....38
Contenido del kit....38
Procedimiento de implementación e instalación....39
7 Actualización de Data Protector for PCs....42
Actualización del servidor Policy Server....42
Actualización de agentes....42
Actualización automática de los agentes mediante la política de actualización de agente....43
Actualización de agente manual....43
8 Cómo obtener soporte técnico para Data Protector for PCs....45
Glosario....46
Índice....49

Acerca de esta guía

Esta guía contiene información acerca de:

- Instalación de HP Data Protector for PCs
- Configuración de las políticas de HP Data Protector for PCs
- Software de agente de HP Data Protector for PCs en los equipos de sobremesa y portátiles de los usuarios
- Determinación de cuántos Agents se pueden admitir
- Obtención de soporte para Data Protector for PCs

Público objetivo

Esta guía está destinada a administradores que desean instalar y configurar HP Data Protector for PCs. A lo largo de su lectura resultará de utilidad tener conocimientos acerca de:

- La administración de Windows

Convenciones y símbolos empleados en este documento

Convención	**Elemento**
Texto en color azul: «Acerca de esta guía» (página 5)	Vínculo de referencia cruzada o dirección de correo electrónico
Texto en color azul y subrayado: http://www.hp.com	Dirección de sitio web
Texto en **negrita**	• Teclas que se deben pulsar • Texto que debe escribirse en un elemento de la interfaz gráfica de usuario (como, por ejemplo, un cuadro) • Elemento de la interfaz gráfica de usuario que se debe seleccionar o en el que se debe hacer clic (como, por ejemplo, un menú, un elemento de una lista, un botón, una pestaña o una casilla de verificación)
Texto en *cursiva*	Texto que se desea destacar

Convención	Elemento
Texto en `monoespacio`	• Nombre de un archivo o un directorio • Texto generado por el sistema • Código • Comando, sus argumentos o los valores de tales argumentos
Texto en *`cursiva y monoespacio`*	• Variables de código • Variables de un comando
Texto en **`negrita y monoespacio`**	Texto en monoespacio que se desea destacar

IMPORTANTE: Estas notas proporcionan información aclaratoria o instrucciones específicas.

NOTA: Estas notas proporcionan información complementaria.

Información general

Si desea obtener información general acerca de Data Protector for PCs, visite el sitio web http://www.hp.com/go/dataprotector.

HP, soporte técnico

Si desea obtener información acerca de soporte técnico internacional, consulte el sitio web de soporte de HP:

http://www.hp.com/support

Reúna la siguiente información antes de ponerse en contacto con HP:

- Nombre de modelo y números del producto
- Número de registro de soporte técnico (si corresponde)
- Número de serie del producto
- Mensajes de error
- Tipo de sistema operativo y nivel de revisión
- Preguntas detalladas

Servicio de suscripción

HP recomienda registrar el producto en el sitio web de Subscriber's Choice for Business:

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

Tras el registro, recibirá notificaciones por correo electrónico acerca de mejoras del producto, nuevas versiones de los controladores, actualizaciones de firmware y otros materiales relacionados con el producto.

Sitios web de HP

Si desea obtener información complementaria, visite los siguientes sitios web de 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

Comentarios acerca de la documentación

HP está abierta a recibir comentarios.

Si desea transmitir algún comentario o sugerencia acerca de la documentación de un producto, envíe un mensaje a la dirección **DP.DocFeedback@hp.com**. Toda información recibida pasará a propiedad de HP.

1 Aspectos generales y requisitos previos

Aspectos generales de Data Protector for PCs

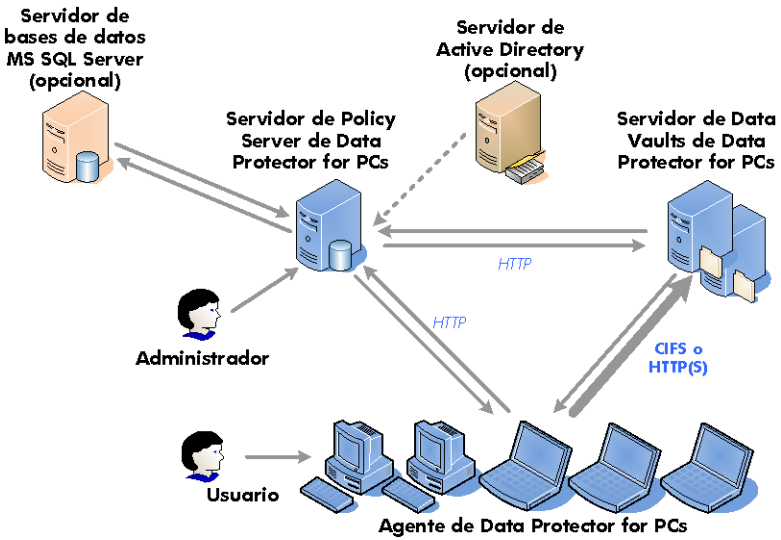
HP Data Protector for PCs consta de dos componentes de software principales: Policy Server y los agentes. Policy Server se ejecuta en un servidor Windows; consulte en la tabla de compatibilidad las versiones compatibles (https://h20230.www2.hp.com/selfsolve/manuals). Los agentes se ejecutan en segundo plano en cada equipo de sobremesa o portátil.

Policy Server también puede acceder a los grupos y unidades organizativas incluidas en un servidor Active Directory.

Los datos de los usuarios se almacenarán en copias de seguridad en Data Vaults. El servidor de Data Vaults debe estar separado del servidor Policy Server. Si está usando los Data Vaults basados en recursos compartidos de archivos de Windows en lugar de los Data Vaults web recomendados, estarán situados en uno o varios recursos compartidos e archivos de Windows en los servidores de archivos.

La arquitectura de Data Protector for PCs se ilustra en el siguiente diagrama:

Figura 1 Arquitectura de Data Protector for PCs



Varias políticas controlan de qué archivos se hace la copia de seguridad desde los equipos de sobremesa y portátiles y dónde se guardan esas copias de seguridad. Las define a través del módulo Policy Server Console. Las políticas se distribuyen automáticamente a los agentes, utilizando el protocolo SOAP sobre HTTP puerto 80. Las políticas se guardan en el Policy Server.

Los agentes ejecutan esas políticas. Cuando un usuario cambia un archivo de datos protegido de acuerdo con esas políticas, se crea una versión anterior en el disco duro local del equipo de sobremesa/portátil y los cambios en el archivo se comprimen y copian a todos los Data Vaults aplicables.

Cada vez que se hace una copia de seguridad de los archivos, el agente notifica a Policy Server, que incluye un historial de auditoría de los cambios en los archivos realizados por los usuarios. Adicionalmente, cada agente envía periódicamente información del "estado" al Policy Server. Puede generar informes de estos datos con el módulo Policy Server Console.

Los Data Vaults se almacenan en el servidor de Data Vaults. Los datos de los clientes se copian a los Data Vaults empleando dos protocolos diferentes: CIFS (para Data Vaults basados en recursos compartidos de archivos de Windows) y HTTP (para Data Vaults web).

El servidor de Data Vaults debe encontrarse instalado en un sistema independiente de aquel en el que se encuentra instalado el servidor Policy Server. El protocolo HTTPS se emplea durante la ejecución del software del servidor web de Data Vaults, junto con el software Cleanup de Data Protector for PCs. En los Data Vaults basados en recursos compartidos de archivos de Windows sólo se instala el software del proceso Cleanup.

Si usa Active Directory, puede configurar Policy Server para acceder a sus grupos y unidades organizativas. Después puede asignar los Data Vaults a los usuarios basándose en su pertenencia a grupos o unidades organizativas. También puede seleccionar los usuarios en los informes basándose en su pertenencia.

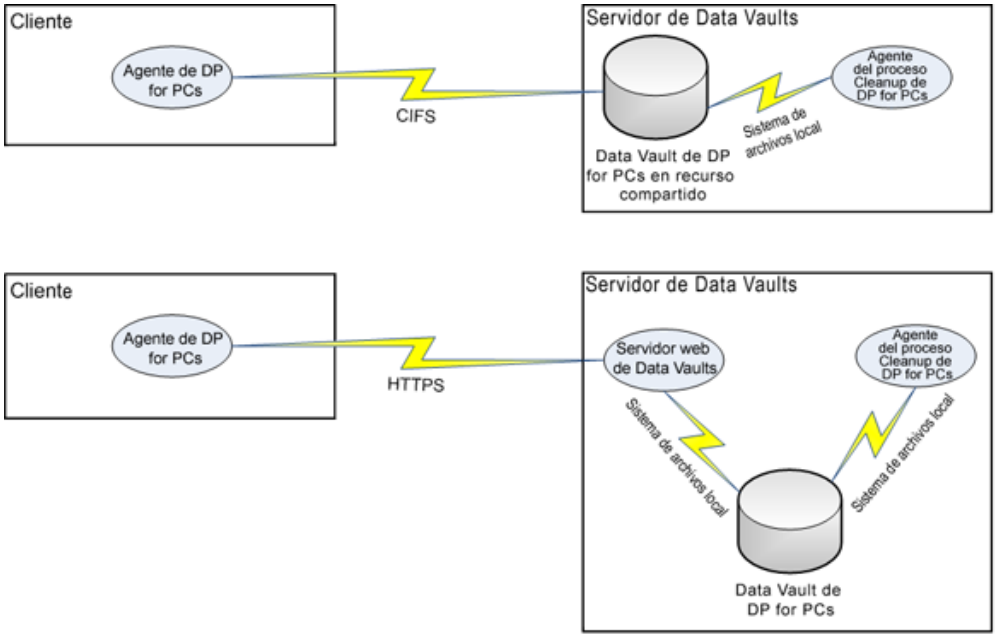
Data Vaults

Existen dos variedades posibles de Data Vaults con Data Protector for PCs:

- Data Vaults web: se basan en el protocolo HTTPS. Proporcionan el máximo nivel de seguridad y el mayor rendimiento en entornos con latencia elevada, por lo que su uso se recomienda.
- Data Vaults basados en recursos compartidos de archivos de Windows: se basan en el protocolo CIFS, que se usaba en versiones anteriores de Data Protector for PCs.

La estructura de datos de ambos tipos de Data Vault es similar, lo cual hace posible convertir un Data Vault basado en un recurso compartido de archivos de Windows en un Data Vault web.

Figura 2 Comparación de Data Vaults basados en web y en recursos compartidos de archivos de Windows



Gestión de certificados

La utilización de SSL es obligatoria para los Data Vaults web. El tipo de certificado se determina durante la instalación del Data Vault web. Para proporcionar un producto que pueda funcionar directamente como viene de serie, por ejemplo, con fines de evaluación, puede instalar el servidor web de Data Vaults con un certificado autofirmado. No es tan seguro como un certificado emitido por una autoridad de confianza (CA). Para conseguir una seguridad total, debería importar un certificado para el servidor de Data Vaults firmado por una autoridad de confianza en su entorno y agréguelo al componente del servidor.

Certificados autofirmados

Al crear una política de Data Vaults, puede definir si se permite un certificado autofirmado. En este caso, no hay que hacer nada en el agente. Un certificado autofirmado emitido por la instalación está limitado a 20 años.

Certificados importados

El procedimiento de importación espera un único archivo en formato PEM, que contenga tanto la clave privada como el certificado coincidente, incluida la clave pública. Tenga en cuenta que el archivo se copia tal cual en el directorio de configuración del servidor web de Data Vaults. En función del procedimiento usado para crear el archivo de certificados, este puede cifrarse. En este caso, el proceso del servicio Windows que se

ejecuta en el servidor web de Data Vaults emitirá un aviso interactivo para obtener la contraseña de descifrado. Esto ocurrirá durante la instalación y también cada vez que el servicio se reinicie en el futuro, por ejemplo, después de un reinicio del sistema. Aunque es posible que pueda agregar esta contraseña manualmente al archivo de configuración del servidor web para evitar el aviso, el proceso de instalación no lo admite. No es aconsejable tener un archivo de certificados cifrado y guardar la contraseña en un archivo junto a él.

NOTA:
El término "autoridad de confianza" implica que los equipos cliente que ejecutan los agentes considerarán que esta autoridad certificante es de confianza y acepta certificados firmados por ella. Se asume que los almacenes de certificados de Windows de los equipos cliente ya se han configurado correctamente añadiendo el certificado de la autoridad certificante y posiblemente certificados adicionales en sus cadenas. El agente no incluye ningún mecanismo para establecer esta confianza. Depende de los mecanismos de Windows.

Intercambio del certificado

Puede intercambiar el certificado en el servidor web de Data Vaults en cualquier momento después de la instalación después de usar la utilidad `DvConfig` descrita en el párrafo CLI «Configuración de las opciones de un Data Vault web desde la interfaz CLI (DvConfig)» (página 21). Por tanto, por ejemplo, puede volver a configurar una instalación configurada inicialmente con un certificado autofirmado para usar un certificado importado.

Aspectos generales de la instalación de Data Protector for PCs

NOTA: Si está actualizando una instalación de Data Protector for PCs, consulte «Actualización de Data Protector for PCs» (página 42).

Hay tres etapas en la instalación de Data Protector for PCs:

1. **Instalar el Policy server de Data Protector for PCs.**

   Consulte «Instalación de Policy Server de Data Protector for PCs» (página 14).

2. **Instalar el software del servidor web de Data Vaults de Data Protector for PCs.**

   Consulte «Instalación, configuración y mantenimiento del servidor web de Data Vaults» (página 18).

3. **Configure las políticas de protección.**

   Consulte «Configuración de las políticas de protección de Data Protector for PCs» (página 23).

4. **Instalar agentes de Data Protector for PCs en equipos portátiles y de sobremesa.**

   Consulte «Instalación de agentes de Data Protector for PCs» (página 37).

Requisitos previos

Policy Server

Para obtener información sobre sistemas operativos admitidos, consulte la tabla de compatibilidad.

NOTA: *Instalación en un sistema operativo Windows 2003 de 64 bits:* Policy Server se ejecuta en modo de compatibilidad de 32 bits en un sistema operativo Windows de 64 bits. Como resultado, Internet Información Services (IIS) debe ejecutarse también en el modo de 32 bits. De no ser así, la instalación lo detectará al verificar los requisitos previos. Le dará entonces la opción de configurar IIS en modo de 32 bits. Si existen otras aplicaciones web instaladas en el servidor que requieran que IIS funcione en el modo de 64 bits (como Microsoft Exchange 2007 con Outlook Web Access), no será posible instalar el servidor Policy Server en el servidor. Este problema no tiene lugar al instalar un servidor Policy Server en Windows 2008.

El servidor debe tener instalado lo siguiente:

- Internet Information Services 6.0, 7.0, 7.5 o posterior, con compatibilidad para aplicaciones ASP.NET.

  En PCs con Windows 2003, IIS 6.0 es un requisito previo y debe encontrarse instalado para poder instalar el servidor Policy Server. En PCs con Windows 2008, Data Protector for PCs ofrece la oportunidad de instalar IIS 7.0 o 7.5 si no se encuentra instalado.

- Microsoft ASP.NET 2.0.

También necesita tener lo siguiente instalado en el servidor.

- Microsoft Installer 3.1 o posterior (necesario para instalar .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 o posterior. El asistente instalará la versión 2.0 SP1.
- Microsoft SQL Express (si no existe ninguna otra versión de SQL instalada).

Además, solo para Internet Information Services 7.0 y 7.5, se necesitan los componentes IIS siguientes. Si no están instalados, el asistente le dará la oportunidad de instalarlos:

- Servidor web de contenido estático de IIS: necesario para prestar servicio a archivos, documentos e imágenes html estáticos
- IIS ASP.NET: necesario para implementar ASP.NET 2.0 y .NET Framework
- Seguridad de IIS: necesario para usar la autenticación integrada de Windows, usada por la consola Policy Server.
- Compatibilidad de gestión de IIS 6: para permitir la configuración de IIS 6 y IIS 7 de la misma forma, en la medida de lo posible.

Base de datos

Data Protector for PCs requiere acceso a una base de datos de Microsoft SQL Server. Consulte la tabla de compatibilidad para obtener información sobre las versiones compatibles.

Puede verificar (y cambiar) el modo de autenticación de la instalación de SQL Server usando Microsoft Enterprise Manager:

1. Haga clic con el botón secundario en la instancia de SQL Server, elija **Propiedades** y haga clic en la pestaña **Seguridad**.
2. Ya se debería haber seleccionado la opción **SQL Server y Windows** (en lugar de la opción **Solo Windows**). Si no lo está, selecciónela y haga clic en **Aceptar**.

Además, durante la instalación de Data Protector for PCs, puede instalar una instancia de SQL Server Express Edition de Microsoft.

Data Protector for PCs Servidor web de Data Vaults

- El servidor web de Data Vaults debe encontrarse instalado en un sistema independiente de aquel en el que se encuentra instalado el servidor Policy Server. (Es posible instalarlo en el mismo sistema, pero esto solo es adecuado con fines de evaluación.)
- Debería instalarse Java Runtime Environment versión 1.6 o posterior.
- Las variables `JAVA_HOME` y `JRE_HOME` deben apuntar al directorio de instalación de Java Runtime.

Agentes de Data Protector for PCs

El software del agente de Data Protector for PCs se puede instalar en los equipos de sobremesa y portátiles de los usuarios que ejecutan Windows. Para obtener información sobre plataformas admitidas, consulte la tabla de compatibilidad.

2 Instalación de Policy Server de Data Protector for PCs

NOTA: Puede actualizar una instalación de Policy Server de Data Protector for PCs a una versión más reciente siguiendo el procedimiento de instalación estándar. Consulte «Actualización del servidor Policy Server» (página 42) si desea obtener más información.

Instalación rápida

Consulte «Policy Server» (página 12) para obtener información sobre los requisitos de Policy Server de Data Protector for PCs.

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Si el asistente para instalación no se inicia automáticamente, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Siga las instrucciones que aparecerán en la pantalla.
3. Policy Server de Data Protector for PCs requiere acceso a una base de datos de Microsoft SQL Server. Seleccione **Usar una instancia existente de Data Protector for PCs de Microsoft SQL Server Express** o haga clic en **Utilizar una instancia existente de Microsoft SQL Server** . Si elige utilizar un servidor SQL existente, tiene que proporcionar la cadena de conexión del servidor de la base de datos y las credenciales para una cuenta con privilegios suficientes para crear una nueva base de datos.
4. Haga clic en **Instalar** en la página **Instalar Policy Server de Data Protector for PCs** del asistente para comenzar la instalación.
5. Una vez finalizada la instalación, haga clic en **Siguiente**. Si lo desea, ejecute la consola Policy Server Console de Data Protector for PCs.
6. Instale el servidor web de Data Vaults en un sistema independiente. Haga clic en **Instalar Data Vault** en la pantalla de instalación principal.

NOTA: Durante la instalación, el software Cleanup siempre se instala junto con el software de servidor web de Data Vaults. Para un servidor de Data Vaults que aloja sólo Data Vaults que dependen de recursos compartidos de archivos de Windows, se recomienda instalarlo localmente en Data Vault para optimizar el rendimiento.

Instalación detallada

NOTA:
Solo Windows 2003 Server: Puede instalar únicamente el Policy Server de Data Protector for PCs desde un CD-ROM compartido en la red o desde un recurso compartido de archivos de la red si la directiva de seguridad en tiempo de ejecución de .NET 2.0 Framework para este servidor está establecida en *Plena confianza* para la zona de seguridad de intranet local. Si el servidor no dispone de una unidad CD-ROM local, cambie la directiva de seguridad en tiempo de ejecución para la zona de seguridad de intranet local a *Plena confianza* usando la herramienta de configuración de .NET Framework 2.0 en Herramientas administrativas, o copie la carpeta Server del CD a un disco local en el servidor.

Tiene que haber iniciado sesión en una cuenta con privilegios de "administrador" para realizar la instalación de Policy Server de Data Protector for PCs.

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Si el asistente para instalación no se inicia automáticamente, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Haga clic en **Instalar Policy Server**.

   Si se le pregunta, seleccione **Abrir** (o **Ejecutar**) este programa desde su ubicación actual en lugar de **Guardar este programa en disco**.
3. El Policy Server de Data Protector for PCs requiere .NET Framework 2.0 SP1. Si todavía no está instalado, se le preguntará si desea instalarlo desde el CD-ROM.

   La instalación requiere Windows Installer 3.1, o posterior, por tanto si es necesario se le preguntará si desea instalar Windows Installer 3.1 desde el CD.
4. El asistente para la instalación comprueba que están instalados los demás requisitos previos:
   - Internet Information Services (IIS)
   - ASP.NET 2.0

   Si falta alguno, haga clic en dicho requisito previo en la lista para obtener más información sobre cómo instalarlo.

   Haga clic en **Siguiente**.
5. Instale Microsoft SQL Server.

Para usar una instancia existente de Microsoft SQL Server:

a. Haga clic en **Usar una instancia existente de Microsoft SQL Server**.

b. En el campo **Servidor de bases de datos**, introduzca la cadena de conexión al servidor de bases de datos existente.

c. En los campos **Nombre de inicio de sesión** y **Contraseña**, introduzca las credenciales para una cuenta con privilegio suficiente para crear una nueva base de datos. Por lo general, será la cuenta "sa".

d. Haga clic en **Siguiente**. La información de conexión que ha introducido se utilizará para realizar una conexión al servidor de la base de datos existente. Si la conexión se realiza correctamente, el asistente continúa al paso 6.

Para instalar la instancia de Data Protector for PCs de Microsoft SQL Server Express Edition:

a. Seleccione **Instalar una instancia de DataProtectorNE de Microsoft SQL Server Express** y haga clic en **Siguiente**.

b. Haga clic en **Instalar** para instalar una instancia de Microsoft SQL Server 2005 Express Edition denominada “DataProtectorNE”. Haga clic en **Siguiente** cuando se complete la instalación.

6. Instalar el software Policy Server de Data Protector for PCs

a. En la pantalla de bienvenida, haga clic en **Siguiente** para comenzar la instalación.

- La consola Policy Server Console de Data Protector for PCs se instalará como aplicación web en el directorio virtual `C:\Inetpub\wwwroot\dpnepolicy`.
- El servicio web de Data Protector for PCs se instalará en `C:\Inetpub\wwwroot\dpnepolicyservice`.

Ambos usan el protocolo HTTP en el puerto 80.

b. Haga clic en **Cerrar** y en **Siguiente** cuando finalice la instalación de Policy Server.

7. Ahora tiene que instalar el programa Cleanup. Haga clic en **Instalar** para comenzar la instalación.
8. Una vez finalizada la instalación del programa Cleanup, haga clic en **Siguiente**.

Puede administrar Data Protector for PCs centralmente desde la consola Policy Server Console de Data Protector for PCs. Como la consola está basada en explorador, puede gestionar Data Protector for PCs desde cualquier equipo que pueda establecer una conexión del explorador al servidor Policy Server (usando HTTP puerto 80).

Para ejecutar la consola Policy Server Console de Data Protector for PCs desde un explorador en el servidor Policy Server, active la casilla de verificación **Ejecutar Policy Server Console** y haga clic en **Finalizar**.

NOTA: Durante la instalación, el software Cleanup se instala en el servidor Policy Server. También se recomienda que lo instale en los Data Vaults para optimizar el rendimiento.

NOTA:

Configuración del explorador para Policy Server Console: Si experimenta algún problema durante la visualización de las páginas de la consola Policy Server Console en el explorador, compruebe su configuración de seguridad. La consola presenta los siguientes requisitos:

- JavaScript debe estar habilitado.
- El bloqueador de ventanas emergentes debe estar deshabilitado para el sitio web de dpnepolicy.
- Puede que sea preciso modificar la configuración de otros parámetros de seguridad dependiendo del explorador en cuestión y su versión.

Instalación con Microsoft SharePoint: Si el servidor Policy Server se instala en un servidor en el que Microsoft SharePoint se encuentre en ejecución, podría obtenerse un error 404 ("No se puede encontrar la página") al ejecutar la consola Policy Server Console. El artículo de Microsoft Knowledge Base al que puede accederse a través de la dirección http://support.microsoft.com/kb/828810 describe el problema y cómo resolverlo. Observe que el problema afecta a todas las aplicaciones web ASP.NET y no sólo a Policy Server.

Para poder ejecutar Policy Server en un servidor con SharePoint, es necesario llevar a cabo los pasos descritos a continuación:

1. Utilice las herramientas de administración de SharePoint para crear exclusiones para las dos aplicaciones web de Policy Server: `dpnepolicy` y `dpnepolicyservice`.
2. Modifique los dos archivos `web.config` de Policy Server (`dpnepolicy\web.config` y `dpnepolicyservice\web.config`) para agregar el código XML `<httpHandlers>` y `<trust>` de acuerdo con lo descrito en el artículo de Microsoft Knowledge Base al que se hizo referencia anteriormente.

3 Instalación, configuración y mantenimiento del servidor web de Data Vaults

Instalación y configuración del servidor web de Data Vaults

NOTA: Instale el servidor web de Data Vaults en un sistema independiente de aquel en el que se encuentra instalado el servidor Policy Server. (Es posible instalarlo en el mismo sistema, pero esto solo es adecuado con fines de evaluación.)

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Si el asistente para instalación no se inicia automáticamente, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Haga clic en **Instalar Data Vault**.
3. Elija entre:
   - **Servidor web de Data Vaults** (recomendado). También instala el software Cleanup en el servidor.
   - **Software del proceso Cleanup para el recurso compartido de archivo de Windows Data Vaults**. Seleccione esta opción solo si pretende utilizar Data Vaults basados en recursos compartidos de archivos de Windows.

   Consulte «Data Vaults» (página 9) si desea obtener más información.
4. Siga las instrucciones que aparecen en pantalla para completar la etapa de instalación.
5. Después de obtener una licencia de Policy Server, si está instalando un servidor web de Data Vaults, comenzará a configurar el Data Vault web.

   En la pantalla Configuración del servidor, introduzca el nombre de dominio completo (FQDN) y el puerto SSL del servidor. Necesitará usar el mismo FQDN al configurar la política web de Data Vaults en el Policy Server. Todos los sistemas cliente deben resolver el nombre, en caso contrario, no será posible realizar la copia de seguridad de algunos de ellos en los Data Vaults de este servidor.
6. En la pantalla Configuración del certificado, tiene que elegir entre:
   - Importación de un certificado SSL existente emitido por una autoridad de confianza (CA). Esta es la opción recomendada y proporciona el nivel mayor de seguridad.
   - Creación de un certificado SSL autofirmado. Proporciona un nivel menor de seguridad y solo debería usarse con fines de evaluación.

NOTA: Puede intercambiar el certificado en el servidor web de Data Vaults en cualquier momento después de la instalación después de usar la utilidad `DvConfig`. Esto incluye la reconfiguración de una instalación con un certificado autofirmado para que utilice un certificado importado. Consulte «Configuración de las opciones de un Data Vault web desde la interfaz CLI (DvConfig)» (página 21).

7. En la pantalla siguiente se le solicita que proporcione los nombres de dos tipos de usuario del servidor web de Data Vaults:
   - **Usuario administrativo**: que supervisa las tareas administrativas, como la creación y eliminación de Data Vaults o la migración de los datos de copia de seguridad de los clientes.
   - **Usuario de copia de seguridad**: que lleva a cabo operaciones propias del usuario final, como la copia de seguridad o la restauración de archivos.

   Estos usuarios son específicos del servidor web de Data Vaults de Data Protector for PCs. Necesitará especificar los detalles de ambos al crear o editar Data Vaults web para este servidor.

   NOTA: Las contraseñas deben tener al menos 8 caracteres.

8. Haga clic en **Siguiente** y, a continuación, en **Finalizar** para completar la instalación y configuración del servidor web de Data Vaults y la instalación del software Cleanup.

Mantenimiento de los Data Vaults web

1. En la página Política de Data Vault, escriba el nombre de dominio completo y el puerto SSL del servidor, así como las credenciales de la cuenta de usuario de copia de seguridad. Haga clic en **Configurar Data Vault** a continuación.
2. Envíe las credenciales de la cuenta de usuario administrativo; se mostrará la página Mantener servidor web de Data Vault.

   Aquí puede seleccionar o eliminar los Data Vaults web existentes. También puede agregar un Data Vault nuevo.

   NOTA: Sólo es posible seleccionar Data Vaults existentes que no se encuentren conectados a otra política de Data Vault.

3. Asegúrese de guardar la política de Data Vault haciendo clic en el botón **Guardar**, situado en la parte inferior de la página.
4. Opcionalmente, si ha agregado un Data Vault nuevo, puede comprobar su existencia y correcta configuración.

Migración de datos de un Data Vault basado en un recurso compartido de archivos de Windows a un Data Vault web

La estructura de los datos de un Data Vault no cambia por tratarse de un Data Vault basado en un recurso compartido de archivos de Windows o un Data Vault web. Como resultado, es posible migrar los datos de un Data Vault de DPNE 6.x existente a un nuevo Data Vault web.

NOTA: Solo es posible efectuar migraciones de datos entre Data Vaults que pertenezcan al mismo servidor Policy Server o compartan la misma contraseña de cifrado.

Existen dos posibles propósitos que justificarían una migración de datos:

- Usar el mismo sistema para hospedar el Data Vault web.

  NOTA: No se admite el acceso en paralelo al mismo directorio a través de un recurso compartido CIFS y un Data Vault basado en web.

- Mover un Data Vault íntegro a otro sistema.

En ambos casos, el servidor web de Data Vaults debe encontrarse instalado localmente en el sistema en el que deban residir los datos.

Para migrar los datos de un Data Vault basado en un recurso compartido de archivos de Windows a un Data Vault web:

NOTA:

- Lleve a cabo la migración en horario no laboral para minimizar el impacto sobre las copias de seguridad en curso.
- Use el Administrador de tareas de Windows para comprobar que el archivo `DPNECleanup.exe` no se encuentre en ejecución.
- Consulte la política de Cleanup en el servidor Policy Server y asegúrese de que la ejecución del archivo `DPNECleanup.exe` no esté programada para desarrollarse durante el periodo de migración.

1. Instale el servidor web de Data Vaults y actualice el servidor Policy Server y los agentes a la versión 7.0. Asegúrese de que todos los agentes se hayan reiniciado tras la instalación de la versión 7.0; sólo entonces podrán comenzar a crear copias de seguridad en el Data Vault web.
2. Deshabilite la política de uso compartido de archivos de Windows que corresponda en la página Política de Data Vault para que los agentes dejen de copiar datos al Data Vault.
3. Si desea usar el mismo directorio para el Data Vault web, detenga el uso compartido del directorio con CIFS.
4. Si el Data Vault web no comparte el servidor con el Data Vault basado en un recurso compartido de archivos de Windows, deberá copiar los datos a una carpeta del

equipo correspondiente cuya ruta de acceso no supere los 67 caracteres. Si el Data Vault reside en el mismo servidor, no será necesario copiar los datos a ninguna otra ubicación, a menos que ello sea preciso por algún motivo.

5. Antes de crear el nuevo Data Vault web, decida cómo deberá llevarse a cabo el proceso de actualización inicial. La actualización inicial se puede omitir si todos los agentes han llevado a cabo una actualización inicial y los datos de copia de seguridad ya se han transferido al Data Vault existente. La opción que permite omitir la actualización inicial no forma parte directa de una política de Data Vault, sino de la política de copia referenciada. Asegúrese de que exista una política de Data Vault configurada correctamente (esto es, con la función de "actualización inicial" desactivada y la configuración de limitación y programación apropiada). Cree una nueva política de copia para esta tarea o modifique una política existente (en cuyo caso resultarán afectadas todas las políticas de Data Vault que hagan referencia a la política de copia modificada).
6. Cree y guarde la nueva política de Data Vault para el Data Vault web. Al crear un nuevo Data Vault web, es preciso especificar la ruta de acceso de una carpeta; en este caso, deberá ser la ruta de acceso en la que residan los datos reales del Data Vault basado en un recurso compartido de archivos de Windows cuya migración esté llevando a cabo. Seleccione la política de copia que creó en el paso 5. Establezca las demás opciones de la política de Data Vault tal y como se encontrasen configuradas en la política del Data Vault basado en un recurso compartido de archivos de Windows original (incluida la configuración de red y Active Directory).
7. Cuando esté seguro de que los agentes estén haciendo correctamente la copia de seguridad de sus archivos en el nuevo Data Vault web, elimine la política del Data Vault basado en un recurso compartido de archivos de Windows.

Una vez guardada la política, los agentes continuarán copiando sus datos en el nuevo Data Vault web empleando el protocolo HTTPS.

Configuración de las opciones de un Data Vault web desde la interfaz CLI (DvConfig)

El uso de esta utilidad desde la interfaz CLI permite cambiar los parámetros de configuración de un Data Vault web (como sus usuarios de copia de seguridad y administrativo, así como sus contraseñas), importar un certificado nuevo, cambiar el puerto SSL y crear un certificado autofirmado nuevo.

Antes de cambiar cualquiera de los parámetros, recuerde detener el servidor web de Data Vaults deteniendo el servicio de Windows HP Data Protector for PCs Data Vault Server.

Una vez aplicados los cambios, reinicie el servicio vinculado a los Data Vaults web. Todas las políticas que hayan sido actualizadas volverán a ser distribuidas a los agentes.

NOTA: Si usa `DvConfig` para cambiar el puerto SSL o el nombre o la contraseña del usuario de copia de seguridad en el servidor web de Data Vaults, asegúrese de cambiar las políticas de Data Vault correspondientes del servidor Policy Server de acuerdo con los cambios.

Uso:

`DvConfig [-adminUser nombre de inicio de sesión:contraseña -backupUser nombre de inicio de sesión:contraseña] [-h] [-i archivo de certificado | -s nombre de host] [-p puerto] [-v]`

`-adminUser nombre de inicio de sesión:contraseña`Establezca las credenciales de la cuenta DvAdmin. Si no se proporciona ningún nombre de inicio de sesión o contraseña, se usará la cadena predeterminada "DvAdmin".

`-backupUser nombre de inicio de sesión:contraseña`Establezca las credenciales de la cuenta DvADvBackup. Si no se proporciona ningún nombre de inicio de sesión o contraseña, se usará la cadena predeterminada "DvBackup".

`–h`
Imprimir este mensaje.

-i *archivo de certificado* Importar un certificado existente.

`-p puerto`Establecer el puerto SSL.

`–s nombre de host`
Crear un certificado autofirmado para el nombre de dominio completo.

`–v`
Imprimir la información de la versión y salir.

4 Configuración de las políticas de protección de Data Protector for PCs

Configuración inicial tras la instalación de Data Protector for PCs

Inmediatamente después de la instalación de Data Protector for PCs, se muestra la ventana Configuración inicial en la consola Policy Server Console. Antes de configurar las políticas para Data Protector for PCs, debe completar correctamente dos pasos de configuración:

1. **Definir o importar una contraseña de cifrado.**

   Para mayor seguridad, tiene que definir una contraseña de cifrado antes de que pueda usar Data Protector for PCs. Esto garantiza que todos los archivos estén cifrados en el ordenador del usuario y se transmitan cifrados a través de la red. Se usa la misma contraseña para cifrar los archivos procedentes de todos los usuarios y para todos los Data Vaults configurados centralmente.

   - Un Data Vault definido centralmente (definido mediante la consola Policy Server Console) siempre usará el cifrado basado en la contraseña de cifrado de Data Protector for PCs.
   - Con los Data Vaults definidos localmente (definidos por los usuarios mediante sus ordenadores), cada uno de los usuarios puede elegir si quiere usar cifrado o no y también elegir sus propias contraseñas.

   La primera vez que instala Data Protector for PCs, tiene que o bien **generar** o bien **importar** una contraseña antes de poder continuar. Después de generar una contraseña, por su seguridad, **exporte** la contraseña. Esto la guarda en una ubicación segura. Más tarde, podrá usarla para importarla.

   Haga clic en **Establecer la Política de cifrado** para gestionar la contraseña y siga las instrucciones que aparecen en la ventana.

   NOTA: Después de generar o importar una contraseña, no puede cambiarla.

2. **Licencia Data Protector for PCs.**

   Si está evaluando Data Protector for PCs, puede usarlo durante 60 días para proteger un número ilimitado de usuarios sin obtener más licencias. Cuando adquiere Data Protector for PCs, tiene que acceder a HP License Key Delivery Service que se encuentra en la dirección URL https://webware.hp.com/welcome.asp, para descargar una clave de licencia que podrá introducir posteriormente. Puede adquirir las siguientes licencias:

   - TA032AA o TA032AAE para 100 agentes
   - TA033AA o TA033AAE para 1.000 agentes

- TA036AA o TA036AAE para 100 agentes más HP Data Protector Starter Pack Windows (B6961BA o B6961BAE)

Tiene que introducir una clave de licencia permanente antes de finalizar el periodo de evaluación. En caso contrario, al final de los 60 días, los agentes ya no podrán copiar los datos a sus repositorios locales o a los Data Vaults. No obstante, aún es posible restaurar las versiones de archivos anteriormente protegidos.

Haga clic en **Gestión de licencias** para gestionarlas y, a continuación, en **Introduzca una clave de licencia para Data Protector for PCs usuarios**. Siga las instrucciones de la ventana.

NOTA: Las licencias se distribuyen a los agentes cuando éstos están instalados.

Después de completar estos pasos de configuración correctamente, dispondrá de todas las funciones de Policy Server Console. Si acaba de instalar Data Protector for PCs, configure otros elementos de Data Protector for PCs en el orden de la sección siguiente.

Configuración por primera vez

Data Protector for PCs viene preconfigurado con unas políticas que suelen bastar para la mayoría de organizaciones. Se le recomienda que configure las políticas de Data Vaults y de copia y protección de archivos en primer lugar y que, a continuación, instale su software de agente Data Protector for PCs en los equipos de sobremesa y portátiles de los usuarios.

NOTA: En lugar de configurar nuevas políticas, puede modificar las políticas que vienen preconfiguradas con Data Protector for PCs. Solo tiene que seleccionar **Editar una política existente** en lugar de **Crear una política nueva** en cada etapa.

Puede configurar las políticas de protección para su instalación desde la consola Policy Server Console. Las políticas que define de manera centralizada se distribuyen a todos los agentes de Data Protector for PCs y se ejecutan en los equipos de sobremesa y portátiles.

1. Ejecute la consola Policy Server Console de Data Protector for PCs al final del asistente para la instalación o en cualquier momento desde un explorador usando la siguiente dirección URL:

   `http://policyserver/dpnepolicy/`

   donde "*policyserver*" es el nombre de su Policy Server de Data Protector for PCs. Debe haber iniciado sesión como "administrador" en el servidor.

2. **Configure las políticas de Data Vault**.

   Las políticas de Data Vault establecen el destino (un Data Vault web o un recurso compartido de archivos Windows) para la realización de copias de seguridad continuas de archivos de usuario protegidos por políticas. Cuando se cambia un archivo, se puede hacer una copia de seguridad automática de la versión anterior

y del archivo editado en uno o más destinos. Cada grupo de usuarios puede asignarse a uno o más Data Vaults. Por ejemplo, puede definir una política de Data Vault llamada *Ventas* y asignarla a sus grupos de usuarios *Dallas.Ventas*, *San Francisco.Ventas*, *Chicago.Ventas* y *Atlanta.Ventas*.

- Un Data Vault definido centralmente (definido mediante la consola Policy Server Console) siempre usará el cifrado basado en la contraseña de cifrado de Data Protector for PCs.
- Con los Data Vaults definidos localmente (definidos por los usuarios mediante su software agente), cada uno de los usuarios puede elegir si quiere usar cifrado o no y también elegir sus propias contraseñas.

NOTA: *Requisitos para todos los Data Vaults:*

Data Protector for PCs establecerá los mismos permisos de acceso (ACL) en los archivos almacenados en copias de seguridad en el servidor de archivos que en el archivo original. Esto significa que los usuarios solo pueden recuperar los archivos almacenados en copias de seguridad si pueden acceder a los archivos originales en sus equipos.

Requisitos para Data Vaults basados en recursos compartidos de archivos de Windows:

Si está usando Data Vaults basados en recursos compartidos de archivos de Windows, los recursos compartidos deberían encontrarse en un servidor de archivos de Windows, que no necesita estar en el mismo equipo que el servidor Policy Server. Sin embargo, si solo está evaluando Data Protector for PCs con un pequeño número de agentes instalados, puede ser útil que Policy Server y el servidor de archivos de Data Vaults estén en el mismo equipo.

Para crear una política de Data Vault:

a. En el panel de navegación de la izquierda, haga clic en **Políticas > Data Vaults > Políticas de Data Vault**.

b. Haga clic en **Crear una nueva política de Data Vault**.

c. Siga las instrucciones de la ventana. El proceso difiere dependiendo del tipo de Data Vault seleccionado (basado en Web o creado a partir de un recurso compartido de archivos de Windows).

NOTA: Cuando cree un Data Vault, la longitud de la ruta de la carpeta o la ubicación compartida no puede ser mayor de 66 caracteres.

Mejores prácticas:

De momento, deje la Política de copia establecida en su valor predeterminado.

Para ejecutar el proceso Cleanup sobre un Data Vault basado en un recurso compartido de archivos de Windows:

- Si el Data Vault está en este Policy Server, mantenga la configuración predeterminada de nombre de este equipo.
- Si el Data Vault está en un servidor de archivos Windows diferente, instale el software de limpieza de Data Vault en él y designe ese equipo como equipo de limpieza (Cleanup).

3. **Configure las políticas de copia**.

   La política de copia establece un límite en el número de clientes que pueden copiar a un Data Vault simultáneamente. También define las actualizaciones iniciales y programadas de los Data Vaults para complementar la copia de seguridad continua. Cada política de copia puede asignarse a uno o más Data Vaults.

   Las políticas de copia definen lo siguiente:

   - Cuántos agentes pueden copiar archivos simultáneamente en sus Data Vaults.
   - Un calendario para las actualizaciones periódicas, que comprueban que existan todos los archivos esperados de un usuario en el Data Vault y, si esto no es así, copian cualquier archivo que falte. Esto proporciona una garantía mayor de que todos los archivos de usuario han sido copiados correctamente al Data Vault.
   - Si debe realizarse una **actualización inicial** (o copia). La actualización inicial es necesaria porque durante las operaciones normales Data Protector for PCs, cada vez que un usuario cambia un archivo Data Protector for PCs que esté continuamente protegido, únicamente se copia la información de los cambios al Data Vault.

   La política de copia predeterminada se aplica a todos los Data Vaults que no tienen establecida una Política de copia explícita. Puede cambiar la configuración de la política de copia predeterminada, pero no eliminarla ni renombrarla.

   Para crear una política de copia:

   a. Haga clic en **Políticas** en el panel de navegación izquierdo.
   b. Haga clic en **Establecer las políticas de copia**.
   c. Haga clic en **Crear una política de copia nueva**.
   d. Siga las instrucciones de la ventana.

   Mejores prácticas:

   - **Limitación**: Establezca el periodo de sus horas de trabajo normales y establezca un límite más bajo para otros periodos.
   - **Actualización inicial**: Habilite la actualización inicial para garantizar que se haga una copia de seguridad de todos los archivos de usuario protegidos por las políticas de protección de archivos.

- **Actualizar archivos cada semana/mes**: Puesto que una actualización debe implicar pocas copias de archivos, si es que hay alguna, habilite las actualizaciones de Data Vault para garantizar que se haga una copia de seguridad adecuada de todos los archivos de usuario protegidos por políticas.

4. **Configure las políticas de protección de archivos**.

   Las políticas de protección de archivos le permiten especificar qué archivos se van a proteger y durante cuánto tiempo se van a conservar las versiones anteriores. Por ejemplo, puede definir una política de protección de archivos llamada *Documentos de Office* para los documentos de Word, las hojas de cálculo de Excel y las presentaciones de PowerPoint.

   Los archivos almacenados en las unidades de disco local se pueden proteger.

   Existen dos tipos de política:

   - **Continuous File Protection**: que proporciona protección en tiempo real a sus archivos cada vez que se guardan en un disco o se eliminan. Por lo general, cualquier archivo o documento que admite la selección del comando **Guardar** en un menú debe protegerse empleando una política de Continuous File Protection.

     Data Protector for PCs incluye varias políticas de ejemplo. De manera predeterminada están seleccionadas tres después de la instalación: *Documentos de Office*, *Desarrollo de software* y *Documentos web*. Puede empezar con estas políticas o crear las suyas.

   - **Open File Protection**: que proporciona protección periódica a los archivos (normalmente, a intervalos de una hora) capturando "instantáneas" de los mismos. Por regla general, cualquier archivo que sea muy grande (más de 100 MB), esté abierto la mayor parte del día o no tenga la opción **Guardar** en el menú debe protegerse con este método. Archivos comunes de este tipo son los archivos de correo electrónico y las bases de datos.

     Data Protector for PCs incluye cuatro ejemplos: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* y *Thunderbird*. Puede empezar con estas políticas o crear las suyas.

     NOTA: Data Protector for PCs no admite la copia de seguridad de archivos cifrados con EFS con políticas Open File Protection, por tanto los archivos como .pst no deben ser cifrados con EFS.

   Para crear una política de protección de archivos:

   a. Haga clic en **Políticas** en el panel de navegación izquierdo.
   b. Haga clic en **Establecer las políticas de protección de archivos**.
   c. Haga clic en **Crear una nueva política de Continuous File Protection** o **Crear una nueva política de Open File Protection**.

d. Siga las instrucciones de la ventana.

NOTA: Cuando cree políticas de protección y establezca reglas de exclusión o inclusión, las extensiones de archivos no pueden tener más de 9 caracteres para las políticas de Open File Protection ni 29 caracteres para las políticas de Continuous File Protection.

En el caso de las políticas de Open File Protection, puede seleccionar archivos sin extensiones en las reglas de inclusión. Esto no es posible para las políticas de Continuous File Protection.

IMPORTANTE: En este momento ya ha configurado todas las políticas básicas que Data Protector for PCs necesita. Data Protector for PCs viene preconfigurado con otras políticas que son suficientes para la mayoría de las organizaciones. Le recomendamos que ahora empiece a instalar los agentes en los equipos de sobremesa y portátiles de sus usuarios (consulte «Instalación de agentes de Data Protector for PCs» (página 37)). Posteriormente, puede volver para revisar y configurar las restantes políticas de Data Protector for PCs, como la política de Cleanup, la política de control por parte del usuario, la política de actualización de agente y la política de retención de datos de informes.

Configuración de las políticas restantes

1. **Configure el acceso a Active Directory**.

NOTA: *Asociación de grupos de Active Directory a Data Vaults:* Es posible asociar Data Vaults a grupos de Active Directory a través de una política de Data Vault. De este modo, todos los miembros pertenecientes a los grupos asociados crearán sus copias de seguridad en el Data Vault asociado. No es posible asociar usuarios individuales. Asimismo, si la asociación se establece con una Unidad de organización (UO), sólo se asociarán los grupos pertenecientes a dicha UO. Los usuarios que pertenezcan directamente a la UO no se asociarán al Data Vault. Puede que, por error, la lista de grupos de Active Directory incluya grupos que no sean de seguridad (como, por ejemplo, grupos de distribución). No obstante, en realidad, sólo se pueden asociar grupos de seguridad a un Data Vault.

Varios usuarios: Si dos o más usuarios están compartiendo un equipo, deben pertenecer al mismo grupo de Active Directory.

Si quiere asignar Data Vaults por grupos o unidades organizativas, o si quiere hacer informes por grupos o unidades organizativas, tiene que configurar Policy Server de tal modo que pueda acceder a su Active Directory.

Al configurar el acceso a Active Directory se habilita la opción **Miembros de grupos seleccionados o unidades organizativas** para los Data Vaults (consulte «Configuración por primera vez» (página 24)).

Para configurar el acceso a Active Directory:

a. Haga clic en **Configuración** en el panel de navegación izquierdo.

b. Haga clic en **Configurar el acceso a Active Directory**.

c. Siga las instrucciones de la ventana.

2. Configure la política de Cleanup.

Los repositorios Local Repository de Data Protector for PCs almacenados en los equipos de los usuarios y los Data Vaults almacenados en los servidores de Data Vaults deben limpiarse periódicamente con objeto de quitar aquellas versiones que no cumplan las condiciones de conservación definidas en las políticas de protección de archivos.

Para configurar la política de Cleanup:

a. Haga clic en **Políticas** en el panel de navegación izquierdo.

b. Haga clic en **Establecer la política de Cleanup**.

c. Siga las instrucciones de la ventana.

Para que el Data Vault pueda admitir más usuarios, ejecute el proceso de limpieza únicamente en fines de semana, empezando el viernes por la tarde o el sábado por la mañana temprano, para que tenga el máximo de tiempo posible para ejecutarse:

a. Abra la página de la Política de Cleanup en la consola de administración del Policy Server y cambie la **Programación de Cleanup de Data Vault**.

b. Desmarque todos los días excepto el viernes o el sábado:

- Para el viernes, elija una hora de inicio a última hora, como las 10 de la noche.
- Para el sábado, elija una hora de inicio a primera hora, como la 1 de la noche.

Con el Cleanup ejecutándose solo los fines de semana:

- La lista de archivos presentados para la restauración desde un Data Vault estarán obsoletos en una semana. Los usuarios siempre pueden desencadenar un nuevo examen manual de sus datos en el Data Vault para obtener una vista actualizada.
- Las versiones de copias de seguridad seguirán existiendo después de su obsolescencia durante una semana porque el proceso Cleanup solo se ejecuta los fines de semana.
- La gestión de la cuota no está actualizada. Si los usuarios exceden su cuota, pueden tener que esperar hasta que el proceso Cleanup se haya ejecutado para volver a tener espacio libre en el Data Vault. Por otro lado, es posible que el sistema no reconozca inmediatamente la cuota porque el informe de uso del espacio forma parte del proceso Cleanup.

Mejores prácticas:

- **Programación de Cleanup del Local Repository**: Deje la opción predeterminada de 1 hora.
- **Programación de Cleanup del Data Vault**: La configuración predeterminada "limpiar todos los días a medianoche" debería ser satisfactoria para la mayoría de instalaciones. Consulte «Recomendaciones de tamaño» (página 32) para obtener más información sobre la capacidad de Data Vault.
- Puede configurar DPNECleanup para usar varios subprocesos de una forma reutilizable y ampliable para un mejor uso de la CPU y del disco, permitiendo que más datos se almacenen. Consulte «Configuración del proceso Cleanup con subprocesos» (página 35).

3. **Configure la política de control por parte del usuario**.

   La política de control por parte del usuario determina cuánto control tienen los usuarios sobre las políticas corporativas distribuidas en sus equipos.

   Para configurar la política de control por parte del usuario:

   a. Haga clic en **Políticas** en el panel de navegación izquierdo.
   b. Haga clic en **Establecer la política de control por parte del usuario**.
   c. Siga las instrucciones de la ventana.

   Mejores prácticas:

   Establezca **permitir control por parte del usuario** para **Recuperación de servicio automático**.

4. **Configure la política de actualización de agente**.

   La política designa la versión del agente de Data Protector for PCs que deben usar todos sus equipos de sobremesa y portátiles protegidos por Data Protector for PCs, que se actualizarán automáticamente a esta versión.

   Para configurar la política de actualización de agente:

   a. Haga clic en **Políticas** en el panel de navegación izquierdo.
   b. Haga clic en **Establecer la política de actualización de agente**.
   c. Siga las instrucciones de la ventana.

5. **Configure la conservación de datos de informes**.

   Este ajuste establece cuánto tiempo se conservan los datos con fines de información en cada una de las categorías principales de información.

   Para configurar la conservación de datos de informes:

   a. Haga clic en **Configuración** en el panel de navegación izquierdo.
   b. Haga clic en **Configurar la retención de datos para informes**.
   c. Siga las instrucciones de la ventana.

Otras tareas de configuración

Estas tareas se suelen realizar cuando se instala Data Protector for PCs por primera vez.

Obtenga la licencia del software de Data Protector for PCs.

Si está evaluando Data Protector for PCs, puede usarlo durante 60 días para proteger un número ilimitado de usuarios sin obtener más licencias. Cuando adquiere Data Protector for PCs, tiene que acceder a HP License Key Delivery Service que se encuentra en la dirección URL https://webware.hp.com/welcome.asp, para descargar una clave de licencia que podrá introducir posteriormente.

Para introducir una clave de licencia:

1. Haga clic en **Administración de licencias** en el panel de navegación izquierdo.
2. Haga clic en **Introducir una clave de licencia para usuarios de HP Data Protector for PCs**.
3. Siga las instrucciones de la ventana.

Si tiene múltiples licencias para introducir, puede crear un archivo de texto con una cadena de clave de licencia en cada línea. A continuación, puede importar el archivo usando el campo Importar clave(s) de licencia.

NOTA: Las licencias se distribuyen a los agentes cuando éstos están instalados.

Desplazamiento de licencias

Si necesita cambiar la dirección IP de Policy Server para mover el servidor a otro sistema, o si tiene que mover licencias de un Policy Server a otro, póngase en contacto con el HP License Key Delivery Service en la dirección URL https://webware.hp.com/welcome.asp.

Establecer, importar y exportar una contraseña de cifrado.

Para mayor seguridad, tiene que definir una contraseña de cifrado antes de que pueda usar Data Protector for PCs. Esto garantiza que todos los archivos estén cifrados en el ordenador del usuario y se transmitan cifrados a través de la red. Se usa la misma contraseña para cifrar los archivos procedentes de todos los usuarios y para todos los Data Vaults configurados centralmente.

- Un Data Vault definido centralmente (definido mediante la consola Policy Server Console) siempre usará el cifrado basado en la contraseña de cifrado de Data Protector for PCs.
- Con los Data Vaults definidos localmente (definidos por los usuarios mediante sus ordenadores), cada uno de los usuarios puede elegir si quiere usar cifrado o no y también elegir sus propias contraseñas.

La primera vez que instala Data Protector for PCs, tiene que generar o importar una contraseña antes de poder continuar. Después de generar una contraseña, por su seguridad, exporte la contraseña. Esto la guarda en una ubicación segura. Más tarde, podrá usarla para importarla.

NOTA: Después de generar o importar una contraseña, no puede cambiarla.

Para administrar su contraseña de cifrado:

1. Haga clic en **Políticas** en el panel de navegación izquierdo.
2. Haga clic en **Política de cifrado**.
3. Siga las instrucciones de la ventana.

Determinación de cuántos Agents se pueden admitir

Es difícil dar reglas generales que se apliquen a todos los entornos, por tanto los casos que se indican aquí describen claramente el contexto para el que son válidos los números dados.

Factores que afectan al tamaño

Establecer el tamaño de un entorno de Data Protector for PCs es complejo. Entre los factores técnicos que influyen en el número de usuarios que puede admitir un entorno específico se incluyen los siguientes:

- Energía de procesamiento en el Data Vault (para la consolidación nocturna de los datos de copia de seguridad)
- Red y ancho de banda de E/S en el servidor de Data Vaults
- Espacio en disco en el servidor de Data Vaults
- Tamaño de la base de datos SQL en el Policy Server
- Ancho de banda de la red y energía de procesamiento en el servidor Policy Server

Los factores que pueden generar un cuello de botella en cualquier instalación se determina tanto por los ajustes de la configuración de Data Protector for PCs como por los patrones de uso:

- Número de usuarios en un Data Vault
- Número y tamaño de archivos cubiertos por las políticas de protección configuradas
- Frecuencia de cambio de los archivos protegidos
- Configuración de la conservación de los tipos de archivos protegidos

Recomendaciones de tamaño

Data Vault

Con una programación diaria de limpieza, un Data Vault con un espacio de disco de 14 TB puede admitir una población de usuarios hasta de **3.500** Agents si las características de datos promedio son aproximadamente las siguientes:

- Número promedio de archivos protegidos: 5000

- Tamaño total promedio de archivos protegidos en el disco local: 10 GB
- Tamaño total promedio en el Data Vault (comprimido): 4 GB

Si necesita proteger más datos en promedio que en este ejemplo, si solo se aumenta la capacidad del disco en el Data Vault, quedará más espacio libre para los datos pero el Data Vault ya no podrá completar la consolidación nocturna de los datos de copia de seguridad de forma oportuna. Considere las posibilidades siguientes:

- Ejecute el proceso Cleanup de Data Vault solo durante el fin de semana. Consulte el paso 2 "Configure la política de Cleanup" en «Configuración de las políticas restantes» (página 28) para obtener más información sobre cómo hacerlo. Esto debería aumentar el número de agentes que puede admitir un Data Vault con espacio en disco de 40 TB a 10.000, dado las mismas características de datos promedio.
- Considere la posibilidad de distribuir datos de usuario final en varios Data Vaults.

Las especificaciones de hardware para tales Data Vaults son las siguientes:

Tipo de Data Vault	Proceso Cleanup diario (hasta 3.500 agentes)	Proceso Cleanup semanal(hasta 10.000 agentes)
Recurso compartido de archivos de Windows	3 GHz dual core, 4 GB RAM, 14 TB de espacio en disco	3 GHz doble núcleo, 4 GB RAM, 40 TB de espacio en disco
Data Vault web	3 GHz cuatro núcleos, 4 GB RAM, 14 TB de espacio en disco	3 GHz cuatro núcleos, 4 GB RAM, 40 TB de espacio en disco

Si los usuarios tienen menos datos como promedio, podrá albergar una cantidad mayor de usuarios en un Data Vault.

NOTA: HP recomienda encarecidamente que, para un mejor rendimiento, mantenga el sistema operativo del Data Vault y los datos de copia de seguridad en discos físicamente separados.

Para un mejor rendimiento, el disco del Data Vault debería desfragmentarse con regularidad.

Policy Server

La cantidad de tráfico generado en el Policy Server depende directamente del número de Agents albergados por el servidor. La edición Express de MS SQL Server que se incluye con Data Protector for PCs impone un tamaño máximo de base de datos de 4 GB y no se admiten más de 5.000[1] agentes.

Si debe admitir más de 5.000 Agents en su entorno, puede tener que disponer de servidores Policy Server adicionales o reemplazar MS SQL Express con una versión completa de Microsoft SQL Server. De esta forma, el servidor Policy Server puede escalar

1. Usando la configuración predeterminada para la "notificar la conservación de datos" en Policy Server de 30 días.

fácilmente hasta 50.000 Agents. Si decide usar la versión completa de MS SQL Server, considere la posibilidad de actualizar la memoria principal de Policy Server hasta al menos 3 GB.

Por motivos de rendimiento, el servidor Policy Server debería ejecutarse en un servidor independiente del servidor de Data Vaults. Es posible ejecutarlos en el mismo servidor, pero esto solo se aconseja con fines de evaluación.

Debe haber al menos un Policy Server, pero no es necesario tener el mismo número de Data Vaults y de servidores Policy Server.

Consideraciones de redes

NOTA: Los Data Vaults web no se ven afectados por una latencia elevada. Lo siguiente se aplica únicamente a los Data Vaults basados en recursos compartidos de archivos de Windows.

En general, en los Data Vaults basados en archivos compartidos de archivos de Windows, HP no recomienda realizar una actualización inicial desde los Agents de Data Protector for PCs a los Data Vaults si la latencia de red entre los dos es mayor que 50 ms. Esto se aplica por lo general a oficinas domésticas u oficinas remotas en una conexión WAN lenta. La actualización inicial funcionará pero tardará bastante tiempo.

Si su entorno incluye oficinas en varios sitios y la latencia de red para algunas de ellas es superior a 50 ms, considere la posibilidad de instalar Data Vaults en más de un sitio para que todas las oficinas puedan alcanzar al menos un Data Vault con una latencia de 50 ms o menos.

Cuando la actualización inicial se ha completado, se pueden ejecutar las actualizaciones desde cualquier ubicación en la red corporativa o incluso desde una oficina doméstica. Por lo general son lo suficientemente pequeños para funcionar bien incluso en conexiones de red lentas.

Si la configuración inicial tiene que realizarse a través de una conexión de latencia elevada, puede tardar varios días en completarse, pero puede interrumpirse sin problema. Data Protector for PCs continuará la actualización en el punto donde se detuvo tan pronto como se reconecte al Data Vault.

SUGERENCIA: Si no conoce la latencia que existe entre las oficinas, utilice el comando `ping` desde un equipo en un sitio para hacer un ping a un equipo en otro sitio. Cada ping correcto notificará la latencia.

5 Configuración del proceso Cleanup con subprocesos

El rendimiento de `DPNECleanup` limita la cantidad de datos de usuario en un Data Vault. Puede configurarlo para que use varios subprocesos de una forma que puedan reutilizarse y ampliarse, lo que proporciona un mejor uso de la CPU y el disco y permite almacenar más datos.

Mediante el proceso Cleanup con subprocesos, el argumento '`-s`' del Scheduler lleva a los argumentos predeterminados '`-e -f -u -p -d 1000`', que incluyen el proceso Cleanup con subprocesos de forma predeterminada y un retraso de 1 segundo para el Auto-Adjuster. Si no desea usar estos valores predeterminados; por ejemplo, para deshabilitar la ejecución con subprocesos o para ajustarlos, elimine el argumento '-s' de la llamada del Scheduler y anexe los argumentos CLI individuales.

NOTA:

Aunque puede desear deshabilitar el proceso Cleanup con subprocesos en ciertas circunstancias, se recomienda mantener '`-e -f -u`' como argumentos para la llamada Cleanup en el Data Vault.

Uso de DPNECleanup.exe para la interfaz CLI

El argumento `-p` del archivo ejecutable `DPNECleanup.exe` permite al proceso Cleanup inicializar e iniciar el motor Parallel Engine y, así, habilitar la ejecución de subprocesos. El motor Parallel Engine pone a disposición del usuario siete argumentos de línea de comandos opcionales. El archivo ejecutable DPNECleanup es capaz de recuperar tales argumentos y enviarlos al motor Parallel Engine.

El proceso DPNECleanup se ejecutará en modo serie si no se establece el argumento `-p`. En tal modo, el motor Parallel Engine no se usa en absoluto.

dpnecleanup

`–a` *`affinity`*

Permite establecer la afinidad de procesador al número indicado, que debe reflejar los bits que establecen el uso de los núcleos de la CPU por parte de los subprocesos.

`–d` *`delay`*

Permite establecer el tiempo en milisegundos que debe transcurrir antes de que el Auto-Adjuster comience a funcionar; de este modo, el motor Parallel Engine tendrá tiempo de iniciar un determinado número de subprocesos y crear un cierto nivel de uso del sistema. De forma predeterminada, el argumento `–s` aplica un retraso de 1000 milisegundos (esto es, 1 segundo).

`–m` *`maxCpuUsage`*

Permite establecer el nivel máximo de uso de la CPU (en todos los núcleos definidos por medio del parámetro `affinity`) a un porcentaje equivalente al valor del parámetro *`maxCpuUsage`*, el cual tratará de respetar el Auto-Adjuster. El valor del parámetro

maxCpuUsage debe ser un número entero comprendido entre 1 y 100. El valor predeterminado es '0' (destinado a deshabilitar la limitación o permitir el uso completo de la CPU).

`-o`

Permite mantener constante el uso de los recursos deshabilitando el Auto-Adjuster y evitando que el motor Parallel Engine modifique el número de subprocesos concurrentes. Use el argumento `-r` para ajustar el número de subprocesos concurrentes. Los argumentos `-d`, `-m` y `-q` se ignoran cuando la ejecución se lleva a cabo empleando el argumento `-o`.

`-p`

Permite habilitar la ejecución del proceso Cleanup empleando subprocesos.

`-q` *maxQueueLength*

Permite establecer el valor máximo de la longitud media de la cola de discos, el cual tratará de respetar el Auto-Adjuster. El valor debe ser un número de punto flotante. El valor predeterminado es 2.0.

`-r` *resourceCount*

Permite establecer el número de recursos concurrentes (subprocesos) al número indicado. De forma predeterminada y en combinación con el argumento `-o`, el sistema trabajará con 2^(número de CPU) subprocesos concurrentes. Si el Auto-Adjuster se encuentra en ejecución, el valor indicado representará el límite de recursos concurrentes expresado en subprocesos. El valor predeterminado del límite es '0', (destinado a deshabilitar la limitación).

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

Permite establecer la prioridad de proceso de todos los subprocesos. El valor predeterminado es `Normal`.

`-s`

Proceso Cleanup de servidor. Permite establecer el proceso Cleanup para todos los Data Vaults, ya hayan sido definidos centralmente o por un usuario. Si la ejecución de subprocesos se encuentra habilitada, este argumento se sustituirá por los argumentos '`-e -f -u -p -d 1000`' al ejecutar el comando.

`-e`

Proceso Cleanup empresarial. Permite establecer el proceso Cleanup para todos los Data Vaults definidos centralmente por las políticas del servidor Policy Server.

`-f`

Proceso Cleanup rápido. Normalmente, el proceso Cleanup de un agente sólo se ejecuta si el sistema se encuentra en estado de inactividad. Esta opción permite iniciar el proceso Cleanup en cualquier momento.

`-u`

Proceso Cleanup definido por el usuario. Permite establecer el proceso Cleanup para todos los Data Vaults definidos por las políticas locales creadas por el usuario.

6 Instalación de agentes de Data Protector for PCs

NOTA: Las licencias se distribuyen a los agentes cuando éstos están instalados.

Los agentes de Data Protector for PCs pueden instalarse de dos formas:

- Individualmente en cada equipo cliente. Consulte «Instalación de los agentes de Data Protector for PCs en equipos cliente individuales» (página 37).
- Implementado en una empresa desde un servidor de archivos al que pueden acceder todos los equipos cliente. Consulte «Implementación de Agents de Data Protector for PCs en una empresa» (página 38).

Instalación de los agentes de Data Protector for PCs en equipos cliente individuales

Requisitos previos

El software del agente de Data Protector for PCs se puede instalar en los equipos de sobremesa y portátiles de los usuarios en los que se ejecuta Windows. Para obtener información sobre plataformas admitidas, consulte la tabla de compatibilidad.

Tiene que haber iniciado sesión en una cuenta con privilegios de "administrador".

Procedimiento de instalación

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Un asistente para la instalación debería iniciarse automáticamente. De lo contrario, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Haga clic en la opción de **instalar o actualizar el software de agente Data Protector for PCs**. Elija **Abrir** (o **Ejecutar**) si aparece un cuadro de diálogo “Abrir o Guardar”.
3. Si el ordenador del usuario no tiene Microsoft Windows Installer 3.1 o posterior instalador, el asistente le ofrece instalarlo. Cuando aparezca el cuadro de diálogo Actualizar Windows Installer, haga clic en **Aceptar** para instalarlo.
4. Si el ordenador del usuario no tiene Microsoft .NET Framework 2.0 SP1 o posterior instalador, el asistente le ofrece instalarlo. Cuando aparezca el cuadro de diálogo Instalar Microsoft .NET Framework 2.0 SP1, haga clic en **Aceptar** para instalarlo.
5. El asistente instala automáticamente el agente de Data Protector for PCs. Siga las instrucciones que aparecerán en la pantalla. Durante la instalación, se le pide que introduzca los detalles del servidor Policy Server.

6. Una vez finalizada la instalación y la configuración, haga clic en **Finalizar**. Si hay una política Open File Protection establecida en el servidor Policy Server, se le pide que reinicie el sistema.

   Ahora debería ver un icono de Data Protector for PCs en la bandeja del sistema (uno de estos, según el estado de la protección: ).

7. Compruebe que el agente de Data Protector for PCs funciona correctamente:
   a. Seleccione o cree un archivo de prueba como un documento de Word o una hoja de cálculo de Excel; por ejemplo, en el escritorio. Realice un par de cambios en él y haga clic en **Guardar**.
   b. Haga clic con el botón secundario en el archivo de prueba en el escritorio, en el Explorador de Windows o en un cuadro de diálogo Abrir. Debería ver tres entradas de Data Protector for PCs en el menú que aparece (**Buscar y recuperar archivos...**, **Copiar versión** y **Abrir versión con *XXX*...**).
   c. Seleccione **Abrir versión con *XXX*...** y debería ver una lista de las versiones con sello de fecha del documento que acaba de crear o modificar. Si selecciona una de las versiones, se abrirá como un documento de sólo lectura en la aplicación adecuada. De esta forma, un usuario recupera una versión anterior de sus documentos desde el repositorio local de Data Protector for PCs.
8. Repita los pasos 1 a 8 para los ordenadores portátiles y de sobremesa de otros usuarios que desee proteger mediante Data Protector for PCs.

Implementación de Agents de Data Protector for PCs en una empresa

Puede implementar Agents de Data Protector for PCs en una empresa mediante el kit de implementación de Agents de Data Protector for PCs, incluido en el CD-ROM de instalación.

NOTA: En PCs con Windows Vista, el uso del kit de implementación no es posible si la función UAC (Control de cuentas de usuario) está habilitada. Para solventar lo anterior, es posible deshabilitar la función UAC o instalar el agente interactivamente.

En el procedimiento descrito a continuación, primero copie el kit de implementación de Agents de Data Protector for PCs que se encuentra en *CD-ROM*:`\Agent` en un directorio de un servidor de archivos al que puedan acceder todos sus usuarios. A continuación, cree un archivo de parámetros en ese directorio mediante `SetupConfig.exe`. Por último, establezca un mecanismo para ejecutar `StartInstall.exe` en el directorio compartido del ordenador de cada usuario. Por ejemplo, puede usar una secuencia de comandos de inicio de sesión. A continuación, puede comprobar su implementación mediante el informe de implementación del Agent en la consola Policy Server Console de Data Protector for PCs.

Contenido del kit

El kit de implementación de Data Protector for PCs incluye los siguientes componentes:

`SetupConfig.exe`	Crea y edita el archivo de inicialización.
`StartInstall.exe`	Inicia `Setup.exe` como un usuario con privilegios.
`Setup.exe`	Instala los requisitos previos y `DataProtectorNE.ini`.
`DataProtectorNE.msi`	Paquete de Windows Installer de Data Protector for PCs para instalar el software del agente.
`DataProtectorNE64.msi`	Paquete de Windows Installer de Data Protector for PCs para instalar el software del agente en equipos de 64 bits.
`DataProtectorNE*.*.mst`	Paquetes de Windows Installer de Data Protector for PCs para instalar el software del agente localizado.
`WindowsInstaller.exe`	Actualizar Windows Installer (necesario para instalar .NET).
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	Instala NET Framework 2.0 SP1.
`Setup.ini`	Archivo de parámetros de configuración e instalación de Data Protector for PCs. Este archivo se creará con `SetupConfig.exe` (consulte el paso 4, a continuación).

Procedimiento de implementación e instalación

1. Copie los archivos en el directorio del agente del CD-ROM de distribución en un directorio al que puedan acceder todos los usuarios que deseen usar el kit de implementación de Agents de Data Protector for PCs. Podría ser el directorio de un recurso compartido netlogon común como `\\su_servidor\DPNEDeploy`.
2. Asegúrese de que el recién creado directorio contiene los archivos antes indicados. Puede eliminar todos los demás archivos.
3. Abra una ventana de comandos de DOS (`cmd.exe`) y cambie al directorio (`cd`) creado en el paso 1.
4. Ejecute `SetupConfig.exe` para crear o editar el archivo de parámetros `Setup.ini`. La primera vez que ejecute `SetupConfig.exe`, debe introducir valores para todos los parámetros. Después, puede ejecutar `SetupConfig.exe` varias veces para cambiar los parámetros. Si no desea cambiar un parámetro, simplemente, pulse **Entrar**.

   Los parámetros necesarios son:

   - **Ruta de acceso UNC a los paquetes de instalación**: ruta completa al directorio compartido en el que se copiaron los archivos en el paso 1, como `\\su_servidor\DPNEDeploy`.
   - El nombre del servidor Policy Server de **Data Protector for PCs**. Puede ser un nombre NetBIOS como `SUSERVIDOR`, o un nombre de dominio completo, como `su_servidor.su-empresa.com`.
   - **Nombre de usuario**: nombre de un usuario con privilegios de administrador en los ordenadores que usan el kit de implementación de Agents de Data

Protector for PCs, como miembro del grupo de administradores de dominio. Normalmente es un nombre de usuario completo que incluye el dominio, como `SUEMPRESA\JerryAdmin`.

- **Contraseña**: contraseña asociada al nombre de usuario. Debe escribirla dos veces para confirmarla.

5. En el ordenador cliente, ejecute `StartInstall.exe`; por ejemplo, `\\su_servidor\DPNEDeploy\StartInstall`. A continuación, esto ejecutará `Setup.exe` en segundo plano y con baja prioridad, con el nombre de usuario y la contraseña especificados en `Setup.ini`. Esto puede hacerse como parte de la secuencia de comandos de inicio de sesión. Tenga en cuenta que no puede incluirlo en una secuencia de comandos de arranque porque la cuenta del equipo no tiene suficientes privilegios de red.
6. `Setup.exe` determina si el ordenador cliente admite el uso de Data Protector for PCs. Para obtener información sobre plataformas de Windows admitidas, consulte la tabla de compatibilidad.
7. `Setup.exe` determina si .NET Framework versión 2.0 SP1 está instalado. De lo contrario, lo instalará, tras lo cual puede ser necesario reiniciar el ordenador.
8. `Setup.exe` determina si Data Protector for PCs ya está instalado. Si no lo está, o si la versión está desactualizada, instala Data Protector for PCs.

NOTA:

Cualquier error que se produzca en los pasos 4–7 registrará un mensaje en el servidor Policy Server de Data Protector for PCs y en el registro de eventos de la aplicación en el ordenador local.

Puede comprobar el estado de implementación del Agent mediante la consola Policy Server Console de Data Protector for PCs:

1. Inicie sesión en el módulo Policy Server Console de Data Protector for PCs.
2. Seleccione **Implementar Agent** en **Informes**, en el panel de navegación izquierdo.

   Aparecerá un resumen de la implementación inicial a la fecha actual. Dicho resumen contendrá:

   - Número de máquinas en las que se ha **terminado** la implementación correctamente.
   - Número de máquinas en las que la implementación está **en curso**.
   - Número de máquinas en las que la implementación ha **fallado**.
3. En la columna **Número de máquinas**, haga clic en un número para ver la lista de máquinas que se encuentran en el estado de implementación seleccionado.

   Se mostrará el estado actual de cada máquina. Por ejemplo, si la implementación ha fallado en una máquina concreta, la columna de **información** contendrá el error

correspondiente. Puede obtener información adicional detallada acerca de una máquina haciendo clic en su nombre NETBIOS.

7 Actualización de Data Protector for PCs

Si está actualizando una versión 6.*x* de Data Protector for PCs a 7.0, hágalo en este orden:

1. Actualice el servidor Policy Server a 7.0. Consulte «Actualización del servidor Policy Server» (página 42).
2. Instale el servidor web de Data Vaults. Consulte la instalación de web en «Instalación, configuración y mantenimiento del servidor web de Data Vaults» (página 18).
3. Actualice los agentes a 7.0.

   Puede actualizarlos usando la actualización manual o "silenciosa" mediante la política de actualización de agente. Consulte «Actualización de agentes» (página 42) si desea obtener más información.

Actualización del servidor Policy Server

Puede actualizar una instalación de Policy Server de Data Protector for PCs a una versión más reciente siguiendo el procedimiento de instalación estándar. Todas las configuraciones existentes (la configuración de los Data Vaults, las licencias, etc.) estarán disponibles en la nueva versión.

Actualización del servidor Policy Server:

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Si el asistente para instalación no se inicia automáticamente, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Haga clic en **Instalar Policy Server** en el cuadro de diálogo de instalación de Data Protector for PCs del asistente para dar paso a la actualización.
3. Siga las instrucciones que aparecerán en la pantalla.
4. Si existe alguna instalación del servidor Policy Server en el equipo, el procedimiento de instalación la detectará y ofrecerá la posibilidad de actualizarla.
5. Siga las instrucciones que aparecerán en la pantalla.
6. Una vez finalizada la instalación, haga clic en **Siguiente**. Si lo desea, ejecute la consola Policy Server Console de Data Protector for PCs.

NOTA: El software Cleanup deberá actualizarse también si se encuentra instalado en el servidor Policy Server. Es posible hacerlo manualmente o a través de una política de actualización de agente.

Actualización de agentes

Si actualiza la versión del servidor de Data Protector for PCs, los agentes existentes que usen la versión anterior de Data Protector for PCs continuarán funcionando como antes.

Puede actualizarlos usando la actualización manual o “silenciosa” mediante la política de actualización de agente.

NOTA: Después de la actualización, es necesario reiniciar todos los agentes para que puedan usar los nuevos Data Vaults web. Se les pide que lo hagan mediante mensajes en globos en la bandeja del sistema y en la pestaña Resumen del panel Mantenimiento de Data Protector for PCs en sus PCs.

Actualización automática de los agentes mediante la política de actualización de agente

Los agentes pueden actualizarse “silenciosamente” mediante la política de actualización de agente del servidor Policy Server. El paquete de instalación se suministrará automáticamente a todos los clientes conectados y la actualización se completará de forma totalmente automatizada. No se interrumpirá al usuario final.

1. En la consola Policy Server Console, seleccione **Políticas->Política de actualización de agente**.
2. Si acaba de actualizar el servidor Policy Server, el procedimiento de instalación ha cargado un nuevo paquete de actualización de agente. En la consola Policy Server Console, esta nueva versión aún no está seleccionada.

   Seleccione la nueva versión del agente para que la versión esté disponible.
3. Al ajustar la limitación, puede ajustar el número máximo de actualizaciones permitido por minuto.
4. Haga clic en **Guardar Política de actualización de agente**.
5. Ahora los agentes se actualizarán automáticamente a la versión más reciente. También se actualizarán automáticamente los agentes de Cleanup.

NOTA: Puede comprobar el progreso de actualización del agente mediante el informe: “Implementación de los agentes”.

Actualización de agente manual

Un agente de Data Protector for PCs puede actualizarse a una versión más reciente ejecutando el proceso de instalación estándar.

Antes de actualizar el agente a una versión más reciente, asegúrese de que la versión del agente es compatible con la versión del servidor Policy Server de Data Protector for PCs.

1. Inserte el CD-ROM de instalación de Data Protector for PCs. Si el asistente para instalación no se inicia automáticamente, ejecútelo manualmente haciendo doble clic en el archivo `setup.hta` que encontrará en el directorio raíz del CD-ROM de instalación.
2. Haga clic en **Instalar agente** en la página Instalar Data Protector for PCs del asistente para dar paso a la actualización.
3. Siga las instrucciones que aparecerán en la pantalla.

4. Si existe alguna instalación del agente en el equipo, el procedimiento de instalación la detectará y ofrecerá la posibilidad de actualizarla.
5. Siga las instrucciones que aparecerán en la pantalla.

8 Cómo obtener soporte técnico para Data Protector for PCs

Data Protector for PCs incluye un año de mantenimiento. Esto le da derecho a:

- Soporte técnico telefónico para hablar con un técnico.
- Actualizaciones del software del servidor y el Agent de Data Protector for PCs. Puede descargar las versiones más recientes de o una imagen en CD-ROM desde el sitio web de Data Protector. Vaya a http://www.hp.com/go/dataprotector.

Glosario

Active Directory
(Término específico de Windows) El servicio de directorios en una red Windows. Contiene información acerca de recursos en la red y los hace accesibles a los usuarios y aplicaciones. Los servicios de directorios proporcionan una manera fiable de nombrar, describir, localizar, acceder a y gestionar recursos, sea cual sea el sistema físico en el que residan.

actualización inicial
Data Protector for PCs protege de forma continua los archivos a medida que los usuarios los modifican guardando los cambios aplicados a los mismos. Siempre que un usuarui crea un Data Vault nuevo, Data Protector for PCs debe llevar a cabo una actualización inicial de todos los archivos protegidos en el Data Vault. Los usuarios pueden elegir cómo debe llevarse a cabo la actualización inicial (inmediatamente o en segundo plano).

Agent
Software Data Protector for PCs que se ejecuta en cada uno de los equipos de sobremesa/portátiles de los usuarios. Comunica con el servidor Policy Server a través de los servicios web (SOAP y XML) por TCP puerto 80.

archivos protegidos
Un archivo protegido es uno del que Data Protector for PCs hace una copia de seguridad automática. Los tipos de archivo que protege la aplicación se definen a través de las políticas Continuous File Protection y Open File Protection.

consola
La consola basada en explorador es el lugar en el que define centralizadamente las políticas Data Protector for PCs. Tiene que ser miembro del grupo del administrador.

Continuous File Protection
Continuous File Protection es un método Continuous Data Protection que Data Protector for PCs usa para almacenar automáticamente los cambios aplicados a un archivo siempre que este se guarda. Esto es adecuado para los archivos de datos que son guardados por el usuario (en contraposición a los archivos que siempre están abiertos, como las bases de datos o los archivos de Outlook). Cada política Continuous File Protection protege un grupo de archivos relacionados de algún modo. De forma predeterminada, Data Protector for PCs incluye políticas para los tipos de archivo de uso más frecuente, como los documentos de Office y las imágenes. Puede editar estas políticas de protección de archivos o crear las suyas propias. La política también especifica cuánto tiempo se conservan las versiones anteriores de los archivos protegidos.

Data Vault
Existen dos tipos de Data Vaults:

- Data Vaults web. Usan el protocolo HTTPS y proporcionan el máximo nivel de seguridad para la transmisión de datos entre los PCs cliente y el Data Vault y el mayor rendimiento en entornos con latencia elevada, por lo que su uso se recomienda.
- Data Vaults basados en recursos compartidos de archivos de Windows. Son carpetas compartidas de un servidor de archivos en las que se almacenan los archivos de acuerdo con una política de Data Vault. El servidor de archivos debe ser compatible con el protocolo de uso compartido de archivos de Windows (CIFS/SMB). El uso de este tipo de Data Vaults no se recomienda en entornos con latencia de red elevada.

La estructura de datos de ambos tipos de Data Vault es similar, lo cual hace posible convertir un Data Vault basado en un recurso compartido de archivos de Windows en un Data Vault web.

A los usuarios se les pueden asignar una o más políticas de Data Vault, basadas en su grupo o en su participación en su unidad de organización.

Local Repository
El Local Repository es una ubicación de almacenamiento segura en equipos del Agent que se usa para guardar archivos protegidos y cambios en los archivos, habitualmente en el disco duro del sistema. Se trata de un directorio de sistema oculto. Los usuarios pueden recuperar rápidamente una versión previa haciendo clic con el botón secundario en el archivo ubicado en el escritorio, en Windows Explorer o en un cuadro de diálogo abierto. Los archivos protegidos por políticas

Continuous File Protection se conservan en un directorio oculto del equipo local hasta que su periodo de conservación caduca. Los archivos protegidos por las políticas de Open File Protection se guardan temporalmente en al almacén de versiones local, solo hasta que se copien al Data Vault. Habitualmente, la ruta del repositorio Local Repository es `C:\{DPNE}`.

Open File Protection

La Open File Protection hace una copia de seguridad de los archivos que siempre están abiertos, como las carpetas personales de Outlook y muchos archivos de bases de datos, tomando instantáneas periódicas a nivel de archivos. En ocasiones, a esto se le llama "pseudo"-Continuous Data Protection. Una política Open File Protection define la protección para los archivos abiertos, definida por conjuntos de reglas de inclusión y exclusión. Por ejemplo, puede definir una política llamada "Carpetas personales de Outlook" que se aplique a los archivos .pst de Outlook especificando una regla de inclusión con "termina en '.pst'". Si desea excluir los archivos .pst archivados, puede crear una regla de exclusión con "contiene 'archive'". Las políticas también especifican cuánto tiempo se conservan las versiones anteriores de los archivos protegidos. Las políticas Open File Protection se aplican a todos los usuarios.

Policy Server

El servidor Policy Server proporciona la gestión central de políticas de Data Protector for PCs. También recopila información de estado de Agents y proporciona informes sobre su despliegue y funcionamiento.

política

Una política es un conjunto de reglas, definida de manera centralizada en el servidor Policy Server y ejecutada por el Agent en cada equipo de sobremesa/portátil/notebook.

Política de Cleanup

Los periodos de conservación establecidos por las políticas de protección de archivos son puestos en práctica por tareas de limpieza que se ejecutan periódicamente. La frecuencia con la que se ejecutan tales tareas la establece la política de Cleanup. De manera predeterminada, los Local Repositories de los usuarios se limpian cada hora, y cualquier Data Vault definido localmente se limpia una vez al día. La limpieza de los Data Vaults basados en recursos compartidos de archivos de Windows definidos centralmente es responsabilidad de un equipo designado a través de la política de Data Vault y la limpieza de los Data Vaults web es responsabilidad.del software del proceso Cleanup que se ejecuta localmente en el servidor de Data Vaults. La política de Cleanup se aplica a todos los usuarios.

política de control por parte del usuario

Esta policía determina cuánto control tienen los usuarios individuales sobre el software Agent que se está ejecutando en su equipo de sobremesa/portátil/notebook. Puede bloquear el Agentde modo que las políticas estén completamente ocultas para los usuarios, puede permitir que vean las políticas pero no las cambien o puede dejar que añadan políticas propias. Puede establecer el nivel de control en cada política Data Protector for PCs importante por separado. La política de control del usuario se aplica a todos los usuarios.

Política de copia

Las políticas de copia definen lo siguiente:

- Cuántos Agent pueden copiar archivos simultáneamente en sus Data Vaults.
- Un calendario para las actualizaciones periódicas, que comprueban que existan todos los archivos esperados de un usuario en el Data Vault y, si esto no es así, copian cualquier archivo que falte. Esto proporciona una garantía mayor de que todos los archivos de usuario han sido copiados correctamente al Data Vault.
- Si debe realizarse una *actualización inicial*. La actualización inicial es necesaria porque durante las operaciones normales Data Protector for PCs, cada vez que un usuario cambia un archivo Data Protector for PCs que esté continuamente protegido, únicamente se copia la información de los cambios al Data Vault.

Si acaba de instalar Data Protector for PCs, tiene que establecer una política de copia para realizar una actualización inicial de todos los archivos protegidos de sus usuarios.

Usuario administrativo

Un usuario del servidor web de Data Vaults que supervisa las tareas administrativas, como la creación y eliminación de Data Vaults o la migración de los datos de copia de seguridad de los clientes.

Usuario de copia de seguridad

Un usuario del servidor web de Data Vaults que lleva a cabo operaciones propias del usuario final, como la copia de seguridad o la restauración de archivos.

Índice

Símbolos

.NET Framework, 15, 37

A

acceder a Active Directory, 28
Active Directory
  acceder, 28
  asociar grupos a Data Vaults, 28
actualizar
  agentes, 42
  Policy Server, 42
agentes, 8
  actualizar, 42
  requisitos previos, 13
Agents
  cuántos se pueden admitir, 32
archivos cifrados con EFS, 27
ASP.NET, 15
aspectos generales, 8
autoridad de confianza, 11
ayuda
  obtener, 6

B

base de datos SQL
  requisitos previos, 13

C

cambiar SSL, 21
certificados, 10, 18
  intercambiar, 11, 21
certificados autofirmados, 10, 18
certificados importados, 10
clave de licencia
  introducir, 31
Cleanup, política, 29
Cleanup, software, 18
CLI, comandos
  DPNECleanup, 35
  DvConfig, 21
configuración del explorador para Policy Server Console, 17
configurar
  Active Directory, acceso, 28
  Cleanup, política, 29
  Informes sobre conservación de datos, 30
  Open File Protection, políticas, 27
  política de actualización de agente, 30
  política de control por parte del usuario, 30
  políticas de copia, 26
  políticas de Data Vault , 24
  políticas de protección de archivos, 27
  políticas por primera vez, 24
  Servidor web de Data Vaults, 18
  subprocesos, cleanup, 35
consideraciones de tamaño, 32
  Data Vault, 32
  Policy Server, 33
  red, 34
consola
  configuración del explorador, 17
  ejecutar, 16, 24
consola, ejecutar, 16, 24
Contenido del kit de implementación de Agents, 38
Continuous File Protection, políticas, 27
contraseña, 23, 31
contraseña de cifrado, 23, 31, 32
convenciones
  documento, 5
crear
  usuario administrativo, 19
  usuario de copia de seguridad, 19

D

Data Protector for PCs
  arquitectura, 8
  aspectos generales, 8
  instalar agentes, 37
  obtener soporte técnico, 45
Data Vaults
  asociar grupos de Active Directory, 28
  migrar datos, 20
  recomendaciones de servidor, 32
  recurso compartido de archivos de Windows, 9
  requisitos, 25
  web, 9
Data Vaults basados en recursos compartidos de archivos de Windows
  migrar datos desde, 20
Data Vaults de recursos compartidos de archivos, 9
Data Vaults web, 9
  eliminar, 19
  mantener, 19
  migrar datos hacia, 20
desplazar licencias, 31
documentación
  proporcionar comentarios, 7
documento
  convenciones, 5
DPNECleanup, 35
DvConfig, 21

E

eliminar Data Vaults web, 19
equipos de sobremesa, requisitos previos, 13
equipos de usuarios, requisitos previos, 13
equipos portátiles, requisitos previos, 13
evaluar Data Protector for PCs, 23, 31
exportar contraseña de cifrado, 23, 31

F

FQDN, 18

H

HP
  soporte técnico, 6

I

IIS, 15
Implementación de los agentes, informe, 43
implementar
  comprobar progreso, 40
  procedimiento, 39
implementar software del Agent, 38
  comprobar progreso, 40
  procedimiento, 39
importar contraseña de cifrado, 31
Informes sobre conservación de datos, 30
Instalación con Microsoft SharePoint, 17
instalar
  agentes, 37
  aspectos generales, 11
  Cleanup, software, 18
  Policy Server, 14
  Servidor web de Data Vaults, 18
  SQL server, 16
intercambiar certificados, 11
Internet Information Services, 15
introducir una clave de licencia, 31
introducir una contraseña de cifrado, 32

L

licencias
  desplazar, 31
  disponibles, 23

M

mantener Data Vaults web, 19
migrar datos a un Data Vault nuevo, 20
modificar
  usuario administrativo, 21
  usuario de copia de seguridad, 21

O

obtener licencia, 23, 31
Open File Protection, políticas, 27

P

Policy Server, 8
  actualizar, 42
  instalar, 14
  recomendaciones, 33
  requisitos previos, 12
  requisitos previos de la base de datos, 13
Policy Server Console
  configuración del explorador, 17
  ejecutar, 16, 24
Policy Server Console, ejecutar, 16, 24
política de actualización de agente, 30
política de control por parte del usuario, 30
políticas
  Actualización de agente, 30
  Cleanup, 29
  configurar por primera vez, 24
  Continuous File Protection, 27
  Control de usuario, 30
  copia, 26
  Data Vault, 25
  distribución de, 8
  Informes sobre conservación de datos, 30
  Open File Protection, 27
  protección de archivos, 27
políticas de copia, 26
políticas de Data Vault , 24
políticas de File Protection
  Open, 27
políticas de protección de archivos, 27
  Modo Continuous, 27
protocolo HTTPS, 9
público, 5
puerto SSL
  cambiar, 21
  introducir, 18

R

red, consideraciones de tamaño, 34
requisitos previos, 12
requisitos previos de la base de datos, 13

S

Servidor web de Data Vaults, 8
  configurar, 18
  instalar, 18
  requisitos previos, 13
servidores
  archivo, 8
  Política, 8
servidores de archivos, 8
SharePoint
  instalar Policy Server con, 17
sitios web
  HP, 7
  HP Subscriber's Choice for Business, 6

software del Agent
    implementar en una empresa, 38
Software del agente
    instalar, 37
soporte técnico, 6, 7, 45
SQL server
    instalar, 16
subprocesos, cleanup, 35
Subscriber's Choice, HP, 6

T

tabla de compatibilidad, 8

U

usuario administrativo
    crear, 19
    modificar, 21
usuario de copia de seguridad
    crear, 19
    modificar, 21

W

Windows Installer, 15, 37