HP Data Protector for PCs 7.0
Guia de Instalação e Administração

Número de peça HP n/d
Publicado: Junho de 2011
Edição Primeira

Índice

Sobre este guia

Este guia fornece informações sobre:

- A instalação do HP Data Protector for PCs
- A configuração das diretivas do HP Data Protector for PCs
- O software Agente do HP Data Protector for PCs nos desktops e notebooks dos usuários
- Como determinar quantos Agents podem ser suportados
- Como obter suporte para o Data Protector for PCs

Público-alvo

Este guia destina-se a administradores que desejam instalar e configurar o HP Data Protector for PCs. Será útil ter conhecimento de:

- Administração do Windows

As convenções e os símbolos do documento

Convenção	**Elemento**
Texto azul: "Sobre este guia" [5]	Links e endereços de e-mail de referência cruzada
Texto sublinhado, azul: http://www.hp.com	endereços de sites
Texto em **negrito**	• Teclas que são pressionadas • Texto digitado em um elemento da GUI, como uma caixa • Os elementos da GUI que são clicados ou selecionados, como itens de menu e listas, botões, guias e caixas de seleção
Texto em *itálico*	Ênfase do texto

Convenção	Elemento
Texto com `espaçamento uniforme`	• Nomes de arquivos e diretórios • Saída do sistema • Código • Comandos, seus argumentos e os valores dos argumentos
Texto com *`espaçamento uniforme e itálico`*	• Variáveis do código • Variáveis de comando
Texto com **`espaçamento uniforme e negrito`**	Texto com espaçamento uniforme enfatizado

IMPORTANTE Apresenta informações de esclarecimento ou instruções específicas.

NOTA Apresenta informações adicionais.

Informações Gerais

As informações gerais sobre o Data Protector for PCs podem ser encontradas em: http://www.hp.com/go/dataprotector.

Suporte técnico da HP

Para obter informações sobre o suporte técnico internacional, consulte o site de suporte da HP:

http://www.hp.com/support

Antes de entrar em contato com a HP, reúna as seguintes informações:

- Os nomes e números do modelo do produto
- O número de registro do suporte técnico (se houver)
- Os números de série do produto
- As mensagens de erro
- O tipo e o nível de revisão do sistema operacional
- Perguntas detalhadas

Serviço de assinatura

A HP recomenda o registro do produto no site Subscriber's Choice for Business:

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

Após o registro, você receberá uma notificação por e-mail sobre as melhorias do produto, novas versões de drivers, upgrades de firmware e outros recursos do produto.

sites da HP

Para obter informações adicionais, consulte os seguintes sites da 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

Feedback da documentação

A HP aprecia o seu feedback.

Para fazer comentários e sugestões sobre a documentação do produto, envie uma mensagem para: **DP.DocFeedback@hp.com**. As mensagens enviadas se tornarão propriedade da HP.

1 Visão geral e pré-requisitos

Visão geral do Data Protector for PCs

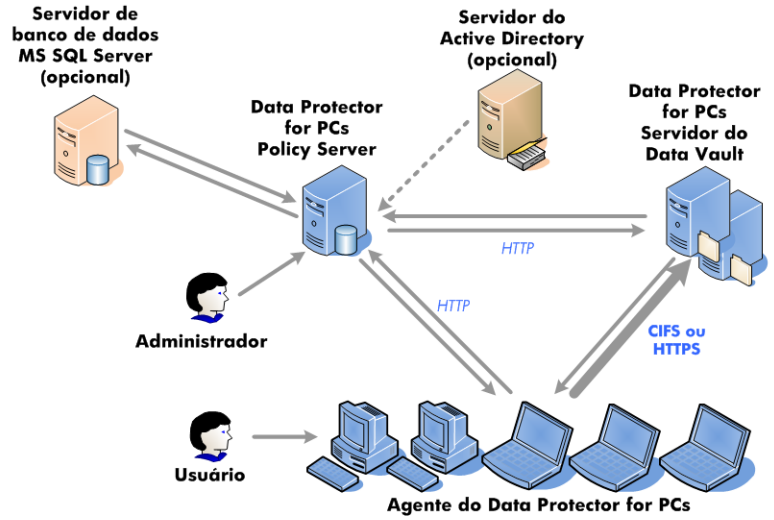
O HP Data Protector for PCs compreende dois componentes de software principais, o Policy Server e os Agentes. O Policy Server é executado no Windows Server; consulte a Matriz de Suporte para conhecer as versões compatíveis (https://h20230.www2.hp.com/selfsolve/manuals). Os Agentes são executados em segundo plano em cada desktop ou notebook.

O Policy Server também pode acessar grupos e unidades organizacionais contidas no servidor de um Active Directory.

O backup dos dados dos usuários é feito nos Data Vaults. O Servidor do Data Vault deve ficar separado do Policy Server. Se você estiver usando Data Vaults de compartilhamento de arquivos do Windows dos Data Vaults Web recomendados, eles ficam em um ou mais compartilhamentos de arquivos do Windows, nos servidores de arquivos.

A arquitetura do Data Protector for PCs é ilustrada no diagrama a seguir:

Figura 1 Arquitetura do Data Protector for PCs



Várias diretivas controlam quais arquivos sofrem backup dos desktops e notebooks, e onde esses backups são mantidos. Você as define através do Console do Policy Server. As diretivas são automaticamente distribuídas aos Agentes, com o protocolo SOAP através da porta 80 do HTTP. As diretivas são mantidas no Policy Server.

Os Agentes executam essas diretivas. Quando um usuário altera um arquivo de dados protegido de acordo com as diretivas, uma versão anterior é criada no disco rígido

local do desktop/notebook e as alterações ao arquivo são comprimidas e copiadas a todos os Data Vaults aplicáveis.

Sempre que backups forem feitos a arquivos, o Agente notifica o Policy Server, que contém um histórico de auditorias das alterações dos arquivos feitas pelas usuários. Além disso, cada Agente envia periodicamente informações sobre a "situação" ao Policy Server. Você pode gerar relatórios desses dados através do Console do Policy Server.

Os Data Vaults ficam no Servidor do Data Vault. Os dados do cliente são copiados para os Data Vaults com diferentes protocolos: CIFS (para Data Vaults do compartilhamento de arquivos do Windows) ou HTTP (Data Vaults Web).

O Servidor do Data Vault deve ficar em um sistema separado do Policy Server. Para o HTTPS, o software do Servidor do Data Vault Web é executado nele, juntamente com o software de Cleanup do Data Protector for PCs. Para os Data Vaults do compartilhamento de arquivos do Windows, o software de Cleanup é instalado nele.

Se você utiliza o Active Directory, pode configurar o Policy Server para acessar seus grupos e unidades organizacionais. Você pode pode atribuir Data Vaults aos usuários, de acordo com sua participação em grupos ou unidades organizacionais. Você também pode selecionar usuários em relatórios, de acordo com sua participação.

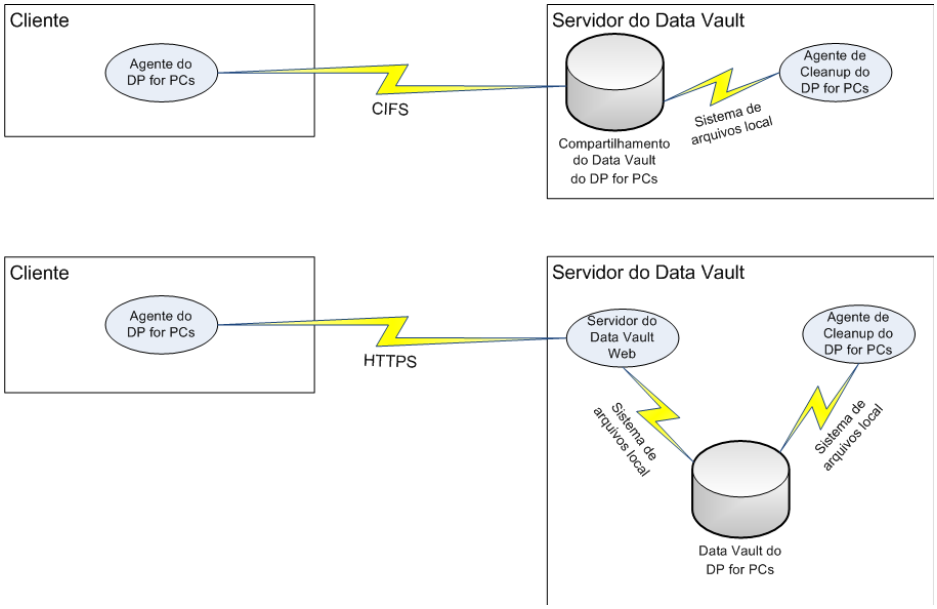
Data Vaults

Há dois tipos de Data Vault possíveis com o Data Protector for PCs:

- Data Vaults Web: baseados no protocolo HTTPS. Proporcionam o melhor nível de segurança e taxa de transferência em ambientes de alta latência, sendo mais recomendados.
- Data Vaults do compartilhamento de arquivos do Windows: baseados no protocolo CIFS, usados em versões anteriores do Data Protector for PCs.

A estrutura de dados desses dois tipos de Data Vault é a mesma, assim, os Data Vaults do compartilhamento de arquivos do Windows podem ser convertidos em Data Vaults Web

Figura 2 Comparação dos Data Vaults Web e do compartilhamento de arquivos do Windows



Manipulação de certificados

A utilização do SSL é obrigatória para os Data Vaults Web. O tipo do certificado é determinado durante a instalação do Data Vault Web. A fim de fornecer um produto que possa funcionar imediatamente, por exemplo, para fins de avaliação, você pode instalar o Servidor do Data Vault Web com um certificado de assinatura automática. Essa assinatura não é tão segura quanto um certificado emitido por uma autoridade confiável (CA) Para dispor de segurança completa, você pode importar um certificado para o Servidor do Data Vault assinado por uma autoridade confiável para o seu ambiente e adicioná-lo ao componente do servidor.

Certificados de assinatura automática

Ao criar uma Diretiva do Data Vault, você pode definir se um certificado de assinatura automática será permitido. Nesse caso, nenhuma ação é necessária no Agente. Um certificado de assinatura automática emitido pela instalação limita-se a 20 anos.

Certificados importados

O procedimento de importação espera um único arquivo no formato PEM, contendo a chave privada e o certificado correspondente, incluindo a chave pública. Observe que o arquivo é copiado para o diretório de configuração do Servidor do Data Vault Web da maneira que está. Dependendo do procedimento usado para a criação do arquivo do certificado, ele pode estar criptografado. Nesse caso, o processo do serviço do Windows executado no Servidor do Data Vault Web emitirá um prompt interativo para

obter a senha de descriptografia. Isso ocorrerá durante a instalação e também a cada vez que o serviço for reiniciado no futuro, por exemplo, após uma reinicialização do sistema. Embora seja possível a adição dessa senha manualmente ao arquivo de configuração do Servidor Web para evitar o prompt, o processo de instalação não suporta essa ação. Não é aconselhável ter de um arquivo de certificado criptografado e armazenar uma senha em um arquivo próximo a ele.

NOTA
O termo "autoridade confiável" sugere que as máquinas clientes que executam os Agentes considerarão essa CA confiável e aceitarão os certificados por ela assinados. Pressupõem-se que os Armazenamentos de Certificados do Windows das máquinas clientes já foram configurados adequadamente com a adição do certificado da CA, e possivelmente outros certificados em suas cadeias. O Agente não inclui qualquer mecanismo para estabelecer essa confiança. Ele confia nos mecanismos do Windows.

Trocando o certificado

Você pode trocar o certificado no Servidor do Data Vault Web a qualquer momento após a instalação, usando o utilitário `DvConfig` descrito no parágrafo do CLI "Configurando as opções do Data Vault Web no CLI (DvConfig)" (página 21). Assim, por exemplo, você pode reconfigurar uma instalação configurada inicialmente com um certificado de assinatura automática para utilizar um certificado importado.

Visão geral da instalação do Data Protector for PCs

NOTA Se você estiver atualizando uma instalação do Data Protector for PCs, consulte "Atualizando o Data Protector for PCs" (página 41).

Há três etapas para a instalação do Data Protector for PCs:

1. **Instalar o Policy Server do Data Protector for PCs.**

   Consulte "Instalando o Policy Server do Data Protector for PCs" (página 14).

2. **Instalar o software do Servidor do Data Vault Web do Data Protector for PCs.**

   Consulte "Instalação, configuração e manutenção do Servidor do Data Vault Web" (página 18).

3. **Configurar as diretivas de proteção.**

   Consulte "Configuração as diretivas de proteção do Data Protector for PCs" (página 23).

4. **Instalar os Agentes do Data Protector for PCs nos notebooks e desktops.**

   Consulte "Instalando os Agentes do Data Protector for PCs" (página 37).

Pré-requisitos

Policy Server

Para sistemas operacionais compatíveis, consulte a Matriz de Suporte.

NOTA *Instalação no sistema operacional Windows 2003 de 64 bits:* O Policy Server é executado no modo de compatibilidade de 32 bits em um sistema operacional Windows de 64 bits. Isso significa que o IIS deve ser executado no modo de 32 bits. Caso contrário, a instalação detectará esse fato durante a verificação dos pré-requisitos. Ela apresentará, então, a opção de definir o IIS no modo de 32 bits. Se houver outros aplicativos Web no servidor que necessitem que o IIS esteja no modo de 64 bits (como o Microsoft Exchange 2007 com Web mail, Outlook Web Access), você não poderá instalar o Policy Server nesse servidor. Essa regra não se aplica à instalação de um Policy Server no Windows 2008.

O servidor deve ter estes itens instalados:

- Internet Information Services 6.0, 7.0, 7.5 ou superior com suporte a aplicativos ASP.NET.

  Para Windows 2003, IIS 6.0 é um pré-requisito e deve ser instalado antes que o Policy Server possa ser instalado. Para o Windows 2008, o Data Protector for PCs oferece a instalação do IIS 7.0 e 7.5, se eles não estiverem instalados.

- Microsoft ASP.NET 2.0

Você também precisa dos seguintes itens instalados no servidor.

- Microsoft Installer 3.1 ou superior (obrigatório para .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 ou superior. O assistente instalará a versão 2.0 SP1.
- Microsoft SQL Express (se nenhuma outra versão do SQL existir)

Além disso, para o IIS 7.0 e 7.5 apenas, os seguintes componentes do IIS são necessários. Se eles não estiverem instalados, o assistente oferecerá a chance de instalá-los:

- IIS Static Content Web Server: necessário para a apresentação de arquivos html estáticos, documentos e imagens
- IIS ASP.NET: necessário para a implantação do ASP.NET 2.0 e do .NET Framework
- IIS Security: necessário para usar a autenticação integrada do Windows, usada para o console do Policy Server.
- IIS 6 Management Compatibility: para permitir que a configuração inicial defina o IIS6 e o IIS 7 da mesma maneira, de acordo com a possibilidade

Banco de dados

O Data Protector for PCs precisa ter acesso a um banco de dados Microsoft SQL Server. Consulte a Matriz de Suporte para conhecer as versões compatíveis.

Você pode verificar (e alterar) o modo de autenticação para a sua instalação do SQL Server usando o Microsoft Enterprise Manager:

1. Clique com o botão direito na instância do SQL Server, escolha **Propriedades** e clique na guia **Segurança**.
2. A opção **SQL Server e Windows**, ao invés da opção **Apenas Windows**, deve estar selecionada. Caso contrário, selecione-a e clique em **OK**.

É possível também, durante a instalação do Data Protector for PCs, instalar uma instância do SQL Server Express Edition da Microsoft.

Servidor do Data Vault Web do Data Protector for PCs

- O Servidor do Data Vault Web deve ser instalado em um sistema diferente do Policy Server. (É possível instalá-lo no mesmo sistema, mas isso só é adequado para fins de avaliação.)
- O Java Runtime Environment versão 1.6 ou posterior deve estar instalado.
- As variáveis `JAVA_HOME` e `JRE_HOME` devem indicar o diretório da instalação do Java Runtime.

Agentes do Data Protector for PCs

O software do Agente do Data Protector for PCs pode ser instalado nos desktops e notebooks dos usuários que possuem Windows. Para conhecer as plataformas compatíveis, consulte a Matriz de Suporte.

2 Instalando o Policy Server do Data Protector for PCs

NOTA Você pode atualizar uma instalação existente do Policy Server do Data Protector for PCs para uma versão mais nova, seguindo o procedimento de instalação padrão. Consulte "Atualizando o Policy Server" (página 41), para obter mais detalhes.

Instalação Rápida

Consulte "Policy Server" (página 12) para obter os requisitos do Policy Server do Data Protector for PCs.

1. Insira o CD-ROM de instalação do Data Protector for PCs. Se o assistente de instalação não for iniciado automaticamente, execute-o manualmente clicando duas vezes em `setup.hta` na raiz do CD-ROM de instalação.
2. Siga as instruções na tela.
3. O Policy Server do Data Protector for PCs precisa ter acesso a um banco de dados do Microsoft SQL Server. Selecione a instância **Usar existenteData Protector for PCs do Microsoft SQL Server Express** ou clique em **Usar uma instância existente do Microsoft SQL Server** . Se você escolher usar um SQL Server existente, precisará fornecer as credenciais e a string de conexão do servidor de banco de dados para uma conta com privilégios suficientes para a criação de um novo banco de dados.
4. Clique em **Instalar** na página **Instalar Policy Server doData Protector for PCs** do assistente para iniciar a instalação.
5. Quando a instalação for concluída, clique em **Avançar** . Você pode escolher executar o Console do Policy Server do Data Protector for PCs.
6. Instale o Servidor do Data Vault Web em um sistema separado. Clique em **Instalar Data Vault** na tela de instalação principal.

NOTA Durante a instalação, o software de Cleanup é sempre instalado juntamente com o software do Servidor do Data Vault Web. Para um Servidor do Data Vault que hospeda apenas Data Vaults de compartilhamento de arquivos do Windows, recomenda-se a sua instalação local no Data Vault, para que o desempenho seja otimizado.

Instalação detalhada

NOTA

Apenas Windows 2003 Server: É possível instalar o Policy Server do Data Protector for PCs apenas de um CD-ROM compartilhado na rede ou de um compartilhamento de arquivos da rede, se a Diretiva de Segurança do Tempo de Execução do .NET 2.0 Framework para esse servidor estiver definida como *Confiança Total* para a Zona de Segurança da Intranet Local. Se o servidor não dispor de uma unidade de CD-ROM local, altere a Diretiva de Segurança do Tempo de Execução para a Zona de Segurança da Intranet Local para *Confiança Total* usando a ferramenta de Configuração do .NET Framework 2.0 nas Ferramentas Administrativas, ou copie a pasta Servidor do CD para um disco local no servidor.

Você precisa estar conectado a uma conta com privilégios de "administrador" para executar a instalação do Policy Server do Data Protector for PCs.

1. Insira o CD-ROM de instalação do Data Protector for PCs. Se o assistente de instalação não for iniciado automaticamente, execute-o manualmente clicando duas vezes em `setup.hta` na raiz do CD-ROM de instalação.
2. Clique em **Instalar Policy Server**.

   Se perguntado, escolha **Abrir** (ou **Executar**) este programa de seu local atual, ao invés de **Salvar este programa no disco**.
3. O Policy Server do Data Protector for PCs exige o .NET Framework 2.0 SP1. Se ele ainda não estiver instalado, você será perguntado se deseja instalá-lo do CD-ROM.

   A instalação exige o Windows Installer 3.1 ou superior, assim, se necessário, você é perguntado se deseja instalar o Windows Installer 3.1 do CD.
4. O assistente de instalação verifica se os outros pré-requisitos estão instalados:
   - Serviços de Informações da Internet (IIS)
   - ASP.NET 2.0

   Se os dois estiverem ausentes, clique nesse pré-requisito na lista para obter detalhes de como instalá-lo.

   Clique em **Avançar**.
5. Instale o Microsoft SQL Server.

   Para usar uma instância existente do Microsoft SQL Server:

a. Clique em **Usar uma instância existente do Microsoft SQL Server**.
b. No campo **Servidor de banco de dados**, insira a string de conexão com um servidor de banco de dados existente.
c. Nos campos **Logon** e **Senha**, insira as credenciais para uma conta com privilégio suficiente para criar um novo banco de dados. Geralmente, essa será a conta "sa".
d. Clique em **Avançar**. As informações de conexão inseridas serão usadas para testar a conexão com o servidor de banco de dados existente. Se a conexão for bem-sucedida, o assistente segue para o passo 6.

Para instalar a instância do Data Protector for PCs do SQL Server Express Edition da Microsoft:

a. Selecione **Instalar a instância do DataProtectorNE do Microsoft SQL Server Express** e clique em **Avançar**.
b. Clique em **Instalar** para instalar a instância do Microsoft SQL Server 2005 Express Edition de nome "DataProtectorNE". Clique em **Avançar** quando a instalação for concluída.

6. Instale o software Policy Server do Data Protector for PCs
   a. Na tela de Boas-vindas, clique em **Avançar** para iniciar a instalação.
      - O Console do Policy Server do Data Protector for PCs será instalado como um aplicativo Web no diretório virtual `C:\Inetpub\wwwroot\dpnepolicy`.
      - O serviço Web do Data Protector for PCs será instalado em: `C:\Inetpub\wwwroot\dpnepolicyservice`.

      Os dois usam o protocolo HTTP na porta 80.
   b. Clique em **Fechar** e **Avançar** quando a instalação do Policy Server for concluída.
7. Agora você precisa instalar o programa de Cleanup. Clique em **Instalar** para iniciar a instalação.
8. Quando a instalação do Cleanup for concluída, clique em **Avançar**.

   O Data Protector for PCs é administrado centralmente no Console do Policy Server do Data Protector for PCs. Como o console é baseado em navegador, você pode gerenciar o Data Protector for PCs de qualquer computador que possa estabelecer uma conexão de navegador com o Policy Server (usando a porta 80 do HTTP).

   Para executar o Console do Policy Server do Data Protector for PCs em um navegador no Policy Server, deixe a caixa de seleção **Executar Console do Policy Server** marcada e clique em **Concluir**.

NOTA Durante a instalação, o software de Cleanup é instalado no Policy Server. Recomenda-se também que ele seja instalado nos Data Vaults, para que o desempenho seja otimizado.

NOTA

Configurações do navegador para o Console do Policy Server: Se você tiver problemas para exibir as páginas do Console do Policy Server em seu navegador, verifique as configurações de segurança do navegador. O Console exige o seguinte:

- O JavaScript deve estar habilitado.
- O bloqueio de pop-ups deve estar desabilitado para o site dpnepolicy.
- Outras configurações de segurança restritivas podem precisar ser modificadas, dependendo de seu navegador ou de sua versão.

Instalação com o Microsoft SharePoint: Quando o Policy Server é instalado em um servidor que utiliza o Microsoft SharePoint, uma mensagem de erro 404 "A página não pode ser encontrada" pode ser exibida quando você executa o Console do Policy Server. O artigo da base de conhecimentos da Microsoft em: http://support.microsoft.com/kb/828810 descreve o problema e sua solução. Observe que esse problema se aplicada a todos os aplicativos Web ASP.NET, não apenas ao Policy Server.

Para que o Policy Server seja executado em um servidor que utiliza o SharePoint, você precisa:

1. Usar as ferramentas de administração do SharePoint para criar exclusões para os dois aplicativos Web do Policy Server. `dpnepolicy` e `dpnepolicyservice`.
2. Modifique os dois arquivos `web.config` do Policy Server (`dpnepolicy\web.config` e `dpnepolicyservice\web.config`) para adicionar o código XML `<httpHandlers>` e `<trust>`, como descrito no artigo da base de conhecimentos da Microsoft citado acima.

3 Instalação, configuração e manutenção do Servidor do Data Vault Web

Instalação e configuração do Servidor do Data Vault Web

NOTA Instale o Servidor do Data Vault Web em um sistema diferente do Policy Server. (É possível instalá-lo no mesmo sistema, mas isso só é adequado para fins de avaliação.)

1. Insira o CD-ROM de instalação do Data Protector for PCs. Se o assistente de instalação não for iniciado automaticamente, execute-o manualmente clicando duas vezes em `setup.hta` na raiz do CD-ROM de instalação.
2. Clique em **Instalar Data Vault**.
3. Escolha entre:
   - **Servidor do Data Vault Web** (recomendado). O software de Cleanup também será instalado no servidor.
   - **Software de Cleanup para o Data Vault do Compartilhamento de Arquivos do Windows**. Selecione essa opção se estiver planejando usar apenas Data Vaults do compartilhamento de arquivos do Windows.

   Consulte "Data Vaults" (página 9), para obter mais informações.
4. Siga as instruções na tela para concluir a fase de instalação.
5. Após obter uma licença do Policy Server, se estiver instalando um Servidor do Data Vault Web, você começará a configurar o Data Vault Web.

   Na tela Configurações do Servidor, insira um nome de domínio totalmente qualificado (FQDN) e a porta SSL do servidor. Você precisará usar o mesmo FQDN durante a configuração da Diretiva do Data Vault Web no Policy Server. O nome deve poder ser resolvido por todos os sistemas clientes, caso contrário, não será possível fazer o backup de alguns deles no Data Vault do servidor.
6. Na tela Configurações do Certificado, é necessário escolher entre:
   - Importar um certificado de SSL existente emitido por uma autoridade confiável (CA). Essa é a opção recomendada, ela oferece o nível mais elevado de segurança.
   - Criar um certificado de SSL de assinatura automática. Essa opção oferece um nível inferior de segurança, devendo ser usada apenas para fins de avaliação.

NOTA Você pode trocar o certificado no Servidor do Data Vault Web a qualquer momento após a instalação, usando o utilitário `DvConfig`. O que inclui reconfigurar uma instalação com um certificado de assinatura automática para que utilize um certificado importado. Consulte "Configurando as opções do Data Vault Web no CLI (DvConfig)" (página 21).

7. A próxima tela solicita os nomes para os dois tipos de usuários do Servidor do Data Vault Web:
   - **Usuário Administrativo**: o responsável pelas tarefas administrativas, como a criação e a exclusão de Data Vaults e a migração dos backups dos dados dos clientes.
   - **Usuário Backup**: responsável por executar operações de usuário final, como o backup e a restauração de arquivos.

   Esses usuários são específicos do Servidor do Data Vault Web do Data Protector for PCs. Será necessário inserir os detalhes dos dois durante a criação ou edição dos Data Vaults Web para esse servidor.

   NOTA As senhas devem ter pelo menos 8 caracteres.

8. Clique em **Avançar**, a seguir, em **Concluir** para concluir a instalação e a configuração do Servidor do Data Vault Web e a instalação do software de Cleanup.

Manutenção dos Data Vaults Web

1. Na página Diretiva do Data Vault, insira o nome de domínio completamente qualificado e a porta do SSL, assim como as credenciais da conta do Usuário de Backup. A seguir, clique em **Configurar Data Vault**.
2. Envie as credenciais da conta do Usuário Administrativo, a página Manter Servidor do Data Vault Web é exibida.

   Nela você pode selecionar ou excluir os Data Vaults Web existentes. Também é possível adicionar um novo Data Vault.

   NOTA Você pode selecionar apenas um Data Vault existente se ele não estiver conectado a outra Diretiva do Data Vault.

3. Certifique-se de salvar a Diretiva do Data Vault clicando em **Salvar** na parte inferior da página.
4. Caso tenha adicionado um novo Data Vault, é possível testar a existência e a configuração adequada do vault.

Migrando dados de um Data Vault existente do compartilhamento de arquivos do Windows para um Data Vault Web

A disposição dos dados em um Data Vault permanece o mesmo tanto para Data Vaults do compartilhamento de arquivos do Windows quanto para o Data Vault Web baseado em HTTPS. Ou seja, você pode migrar os dados de Data Vaults existentes do DPNE 6.x para novos Data Vaults Web.

NOTA A migração de dados pode ser realizada apenas para Data Vaults pertencentes ao mesmo Policy Server ou que compartilham a mesma senha de criptografia.

Há duas situações possíveis para a migração de dados:

- Usar o mesmo sistema para hospedar o Data Vault Web.

  NOTA Acessar o mesmo diretório em paralelo por meio de um compartilhamento de arquivos do Windows e um Data Vault Web não é suportado.

- Mover todo o Data Vault para outro sistema.

Nos dois casos, o Servidor do Data Vault Web deve ser instalado localmente no sistema no qual os dados serão colocados.

Para migrar os dados de um Data Vault existente do compartilhamento de arquivos do Windows para um Data Vault Web:

NOTA

- Execute a migração fora do horário comercial para minimizar o efeito dos backups em execução.
- Observe o Gerenciador de Tarefas do Windows para se certificar de que o `DPNECleanup.exe` não está sendo executado.
- Verifique a Diretiva de Cleanup no Policy Server para se certificar de que o `DPNECLeanup.exe` não esteja agendado para ser executado durante o período de migração

1. Instale o Servidor do Data Vault Web e atualize o Policy Server e os Agentes para a versão 7.0. Certifique-se de que todos os Agentes executaram uma reinicialização após a instalação da versão 7.0, pois só então eles podem dar início ao backup dos dados para o Data Vault Web.
2. Desabilite a diretiva correspondente do compartilhamento de arquivos do Windows na página Diretiva do Data Vault, para que os Agentes interrompam a cópia de dados para o Data Vault.
3. Se você planeja usar o mesmo diretório para o Data Vault Web, cancele o compartilhamento do diretório com o CIFS.
4. Se o Data Vault Web estiver em um servidor diferente do Data Vault do compartilhamento de arquivos do Windows, os dados devem ser copiados para

essa máquina, para uma pasta que não ultrapasse 67 caracteres. Se o Data Vault estiver no mesmo servidor, não há necessidade de copiar os dados para um novo local, a menos que isso seja feito intencionalmente por outros motivos.

5. Antes de criar um novo Data Vault Web, escolha o comportamento do processo de atualização inicial. A atualização inicial pode ser ignorada se todos os Agentes tiverem executado uma atualização inicial, de maneira que o backup dos dados já esteja completo no Data Vault existente. A opção de ignorar a atualização inicial não faz parte da Diretiva do Data Vault, mas da Diretiva de Cópia citada. Certifique-se de que uma Diretiva do Data Vault com a seleção da opção adequada exista (ou seja, com a "atualização inicial" desativada e as configurações de limitação e programação adequadas). Crie uma nova Diretiva de Cópia para ele, ou modifique uma diretiva existente (neste caso, todas as Diretivas do Data Vault referentes à Diretiva de Cópia serão afetadas).
6. Crie e salve a nova Diretiva do Data Vault para o Data Vault Web. Quando você cria um novo Data Vault Web, é preciso fornecer o caminho da pasta e, neste caso, ele será o caminho no qual os dados reais do Data Vault do compartilhamento de arquivos do Windows que você está migrando estão. Selecione a Diretiva de Cópia criada na etapa 5. Defina as outras opções para a Diretiva do Data Vault da mesma maneira que foram criadas na diretiva do Data Vault original do compartilhamento de arquivos do Windows (como as configurações de rede e do Active Directory).
7. Quando tiver certeza de que os Agentes estão fazendo o backup dos arquivos para o novo Data Vault Web, exclua a Diretiva original do Data Vault do compartilhamento de arquivos do Windows.

Após salvar a diretiva, os Agentes reiniciarão a cópia de seus dados para o novo Data Vault Web, usando o protocolo HTTPS.

Configurando as opções do Data Vault Web no CLI (DvConfig)

Utilizar esse utilitário no CLI permite a alteração dos parâmetros de configuração de um Data Vault Web, como os usuários de Backup e Administrativos e suas senhas, importar um novo certificado, alterar o SSL e criar um novo certificado de assinatura automática.

Antes de alterar qualquer parâmetro, você deve desativar o Servidor do Data Vault Web desativando o Servidor do Data Vault do HP Data Protector for PCs de serviço do Windows.

Após fazer as alterações, reinicie o serviço do Data Vault Web. Todas as diretivas atualizadas serão redistribuídas aos Agentes.

NOTA Se você utilizar o `DvConfig` para alterar a porta do SSL ou o nome/senha do Usuário de Backup no servidor do Data Vault Web, certifique-se de alterar as Diretivas do Data Vault correspondentes no Policy Server.

Uso:

`DvConfig [-adminUser logon:senha -backupUser logon:senha] [-h] [-i certificado | -s nome de host] [-p porta] [-v]`

`-adminUser logon:senha`
Defina as credenciais para a conta do DvAdmin. Se não for informado um logon ou uma senha, o padrão "DvAdmin" é usado.

`-backupUser logon:senha`
Defina as credenciais para a conta do DvBackup. Se não for informado um logon ou uma senha, o padrão "DvBackup" é usado.

`–h`
Imprimir essa mensagem.

-i *certificado*
Importar um certificado existente.

`-p porta`Definir a porta do SSL.

`–s nome de host`
Criar um certificado de assinatura automática para o nome de domínio completamente qualificado.

`–v`
Imprimir as informações da versão e sair.

4 Configuração as diretivas de proteção do Data Protector for PCs

Configuração inicial após a instalação do Data Protector for PCs

Imediatamente após a instalação do Data Protector for PCs, a janela Configuração Inicial será exibida no Console do Policy Server. Antes que as diretivas do Data Protector for PCs possam ser configuradas, é necessário executar dois passos de configuração:

1. **Definir ou importar uma senha de criptografia.**

   Por motivos de segurança, você deve definir uma senha de criptografia antes que possa usar o Data Protector for PCs. Isso garante que todos os arquivos estão criptografados no computador do usuário e são transmitidos criptografados pela rede. A mesma senha é usada para criptografar os arquivos de todos os usuários e para todos os Data Vaults configurados centralmente.

   - Um Data Vault definido centralmente (definido através do Console do Policy Server) sempre utilizará a criptografia baseada na senha de criptografia do Data Protector for PCs.
   - Com os Data Vaults definidos localmente (definidos pelos usuários através de seus computadores), cada usuário pode escolher se utilizará a criptografia ou não, e escolher suas próprias senhas.

   Quando você instala pela primeira vez o Data Protector for PCs, você deve **gerar** ou **importar** uma senha antes que possa continuar. Após gerar a senha, para sua segurança, **exporte** a senha. Assim, ela é salva em um local seguro. Você poderá utilizá-la mais parte para importação.

   Clique em **Definir a Diretiva de Criptografia** para gerenciar a senha, e siga as instruções na janela.

   NOTA Após gerar ou importar uma senha, ela não pode ser alterada.

2. **LicençaData Protector for PCs.**

   Se estiver avaliando o Data Protector for PCs, você pode usá-lo por 60 dias para proteger um número ilimitado de usuários sem a necessidade de outra licença. Quando você compra o Data Protector for PCs, você precisa acessar o HP License Key Delivery Service em: https://webware.hp.com/welcome.asp, para baixar uma chave de licença, a qual pode ser inserida posteriormente. Você pode comprar as seguintes licenças:

   - TA032AA ou TA032AAE para 100 Agentes
   - TA033AA ou TA033AAE para 1000 Agentes
   - TA036AA ou TA036AAE para 100 Agentes mais o HP Data Protector Starter Pack Windows (B6961BA ou B6961BAE)

Você deve inserir uma chave de licença permanente antes do fim do período de avaliação. Caso contrário, ao final dos 60 dias, os Agentes não mais poderão copiar dados para seus Local Repositories nem para os Data Vaults. Porém, ainda será possível restaurar as versões de arquivos protegidas anteriormente.

Clique em **Gerenciamento de Licença** para gerenciar o licenciamento, a seguir, clique em **Inserir uma chave de licença para os usuários do Data Protector for PCs**. Siga as instruções na janela.

NOTA As licenças são distribuídas aos Agentes quando os Agentes são instalados.

Após concluir esses passos de configuração, o Console do Policy Server em pleno funcionamento estará disponível a você. Se você acabou de instalar o Data Protector for PCs, configure os outros elementos do Data Protector for PCs na ordem da seção a seguir.

Configurando pela primeira vez

O Data Protector for PCs é fornecido pré-configurado com diretivas suficientes para a maioria das organizações. Recomendamos que as diretivas de Data Vault, Cópia e Proteção de Arquivos sejam configuradas antes e que, a seguir, você instale o software do Agente do Data Protector for PCsnos desktops e notebooks dos usuários.

NOTA Ao invés de configurar novas diretivas, você pode modificar as diretivas pré-configuradas do Data Protector for PCs. Simplesmente selecione **Editar uma diretiva existente**, ao invés de **Criar uma nova política** em cada etapa.

As diretivas de proteção para a sua instalação são configuradas no Console do Policy Server. As políticas definidas centralmente são distribuídas a todos os Agentes do Data Protector for PCs e executadas nos desktops e notebooks dos usuários.

1. Execute o Console do Policy Server do Data Protector for PCs ao final do assistente de instalação, ou a qualquer momento em um navegador usando o URL:

   `http://policyserver/dpnepolicy/`

   onde "`policyserver`" é o nome do Policy Server do seu Data Protector for PCs. Você deve estar conectado como "administrador" no servidor.

2. **Configurar as diretivas do Data Vault**.

   As Diretivas do Data Vault definem o destino (um Data Vault Web ou um compartilhamento de arquivos do Windows) para o backup contínuo dos arquivos dos usuários protegidos por diretivas. Quando um arquivo é alterado, o backup da versão anterior e do arquivo editado podem feitas automaticamente em um ou mais destinos. Cada grupo de usuários pode receber um ou mais Data Vaults. Por exemplo, você pode definir uma diretiva de Data Vault de nome *Vendas* e atribui-la

aos seus grupos de usuários *Dallas.Vendas*, *São Francisco.Vendas*, *Chicago.Vendas* e *Atlanta.Vendas*.

- Um Data Vault definido centralmente (definido através do Console do Policy Server) sempre utilizará a criptografia baseada na senha de criptografia do Data Protector for PCs.
- Com os Data Vaults definidos localmente (definidos pelos usuários através de seu software Agente), cada usuário pode escolher se utilizará a criptografia ou não, e escolher suas próprias senhas.

NOTA *Requisito para todos os Data Vaults:*

O Data Protector for PCs definirá as permissões de acesso (ACL) nos arquivos com backups feitos no servidor da mesma forma que o arquivo original. Isso significa que os usuários podem apenas recuperar os backups de arquivos, se eles puderem acessar os arquivos originais em seus computadores.

Requisito para os Data Vaults do compartilhamento de arquivos do Windows:

Se você estiver usando Data Vaults do compartilhamento de arquivos padrão do Windows, os compartilhamentos devem estar no servidor de arquivos do Windows, que não precisa ser a mesma máquina que o Policy Server. Entretanto, se você está apenas avaliando o Data Protector for PCs com um número pequeno de Agentes instalados, pode ser útil que o servidor de arquivos do Data Vault e Policy Server sejam a mesma máquina.

Para criar uma diretiva do Data Vault:

a. Clique em **Diretivas > Data Vaults > Diretivas do Data Vault** no painel de navegação esquerdo.

b. Clique em **Criar uma nova diretiva do Data Vault**.

c. Siga as instruções na janela. O processo muda se você selecionar um tipo de Data Vault baseado na WEB ou de Compartilhamento de Arquivos do Windows.

NOTA Quando você cria um Data Vault, a extensão do caminho do compartilhamento ou pasta não deve ser maior que 66 caracteres.

Práticas recomendadas:

Deixe a Diretiva de Cópia definida como "Padrão" por enquanto.

Para o Cleanup com Data Vaults do compartilhamento de arquivos do Windows:

- Se o Data Vault não estiver no Policy Server, mantenha as configurações padrão do nome desta máquina.
- Se o Data Vault estiver um um servidor de arquivos diferente do Windows, instale o software de Cleanup do Data Vault nele e atribua essa máquina como a máquina de cleanup.

3. **Configurar diretivas de Cópia**.

A diretiva de Cópia define um limite sobre o número de clientes que podem ser copiados para um Data Vault simultaneamente. Ela também define as atualizações de Data Vault iniciais e agendadas para complementar o backup contínuo. Cada diretiva de Cópia pode receber um ou mais Data Vaults.

As diretivas de Cópia definem o seguinte:

- Quantos Agentes podem copiar arquivos simultaneamente a seus Data Vaults.
- Um agendamento de atualizações periódicas, que verifica se todos os arquivos esperados para um usuários existem no Data Vault e, se não existirem, copia os arquivos ausentes. O que oferece maior garantia de os arquivos de todos os usuários foram adequadamente copiados para o Data Vault.
- Caso uma **atualização inicial** (ou cópia) deva ser executada. A atualização inicial é necessário, pois, durante a operação regular doData Protector for PCs, cada vez que um usuário altera um arquivo protegido continuamente do Data Protector for PCs, apenas as informações sobre as alterações são copiadas para o Data Vault.

A diretiva de Cópia padrão é aplicada a todos os Data Vaults que ainda não possuem uma diretiva de Cópia explícita. Você pode alterar as configurações para a diretiva de Cópia padrão, mas não é possível exclui-la nem renomeá-la.

Para criar uma diretiva de Cópia:

a. Clique em **Diretivas** no painel de navegação esquerdo.
b. Clique em **Definir a Diretiva de Cópia**.
c. Clique em **Criar uma nova diretiva de cópia**.
d. Siga as instruções na janela.

Prática recomendada:

- **Limitação**: Defina o período de tempo para as suas horas de trabalho normais ou defina uma limitação inferior para outros períodos.
- **Atualização inicial**: Habilite a atualização inicial para garantir o backup dos arquivos de todos os usuários protegidos pelas diretivas de Proteção de Arquivos.
- **Atualizar arquivos toda(o) semana/mês**: Como uma atualização necessita envolver poucas, se envolver alguma, cópias de arquivos, habilite as atualizações do Data Vault para garantir o backup de todos os arquivos dos usuários protegidos por diretivas.

4. **Configurar as diretivas de Proteção de Arquivos**.

As Diretivas de Proteção de Arquivos permitem a especificação dos arquivos que serão protegidos e o tempo pelo qual as versões anteriores serão retidas. Por exemplo, você pode definir uma Diretiva de Proteção de Arquivos de nome *documentos do Office* para documentos do Word, planilhas do Excel e apresentações do PowerPoint.

Os arquivos armazenados em unidades de disco locais podem ser protegidas.

Há dois tipos de diretivas:

- **Continuous File Protection**—que fornece proteção em tempo real para os arquivos sempre que eles forem salvos em disco ou excluídos. Geralmente, qualquer arquivo ou documento que permita a você selecionar a opção **Salvar** a partir de um menu deveria ser protegido com uma diretiva de Continuous File Protection.

  O Data Protector for PCs incluem várias diretivas de exemplo. Três são selecionadas por padrão após a instalação: *Documentos do Office*, *Desenvolvimento de Software* e *Documentos da Web*. Você pode começar com essas diretivas ou criar as suas.

- **Open File Protection**—que fornece proteção dos arquivos ao fazer periodicamente um "instantâneo" do arquivo (geralmente uma vez a cada hora). Geralmente, qualquer arquivo que seja muito grande (acima de 100 MB), fique aberto durante a maior parte do dia ou não possua uma opção de menu **Salvar** deveria ser protegido por esse método. Arquivos comuns desse tipo são arquivos de e-mail e bancos de dados.

  O Data Protector for PCs inclui quatro exemplos: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* e *Thunderbird*. Você pode começar com essas diretivas ou criar as suas.

  NOTA O Data Protector for PCs não oferece suporte ao backup de arquivos criptografados por EFS com diretivas de Open File Protection, assim, os arquivos como os .pst não devem ser criptografados por EFS.

Para criar uma diretiva de Proteção de Arquivos:

a. Clique em **Diretivas** no painel de navegação esquerdo.

b. Clique em **Definir as Diretivas de Proteção de Arquivos**.

c. Clique em **Criar uma nova Diretiva de Continuous File Protection** ou **Criar uma nova Diretiva de Open File Protection**.

d. Siga as instruções na janela.

NOTA Quando você cria diretivas de Proteção de Arquivos e define as regras de exclusão e inclusão, as extensões dos arquivos não podem ultrapassar 9 caracteres para as diretivas de Open File Protection e 29, para as diretivas de Continuous File Protection.

Para as diretivas de Open File Protection, você pode selecionar os arquivos sem extensões nas regras de inclusão. Isso não é possível para diretivas de Continuous File Protection.

IMPORTANTE Até agora, você configurou todas as diretivas básicas que o Data Protector for PCs necessita. O Data Protector for PCs é oferecido pré-configurado com outras diretivas que são suficientes para a maioria das organizações. Recomendamos que você comece agora a instalar os Agentes nos desktops e notebooks de seus usuários (consulte "Instalando os Agentes do Data Protector for PCs" (página 37)). Mais tarde, você pode retornar para revisar e configurar as diretivas restantes do Data Protector for PCs, como a Diretiva de Cleanup, a Diretiva de Controle de Usuário, a Diretiva de Atualização de Agente e a Diretiva de Retenção de Dados para Relatórios.

Configuração das diretivas restantes

1. **Configurar acesso ao Active Directory**.

NOTA *Associando grupos de Active Directory a Data Vaults:* Você pode associar Data Vaults com grupos de Active Directory na Diretiva do Data Vault. Todos os membros dos grupos associados sofrerão o backup no Data Vault associado. Você não pode associar usuários individuais. Além disso, se você associar uma Unidade Organizacional (UO), apenas os grupos dentro dessa UO são associados. Qualquer usuário que estiver diretamente na UO não é associado ao Data Vault. A lista de grupos de Active Directory pode incluir incorretamente grupos diferentes dos grupos de segurança, como grupos de distribuição. Porém, apenas os grupos de segurança serão associados ao Data Vault.

Vários usuários: Se dois ou mais usuários estiverem compartilhando um computador, eles devem pertencer ao mesmo grupo de Active Directory.

Se desejar atribuir Data Vaults por grupo ou unidade organizacional, ou se desejar emitir relatórios por grupo ou unidade organizacional, é necessário configurar o Policy Server para que possa acessar o seu Active Directory.

Configurar o acesso ao Active Directory habilita a opção **Membros de grupos e unidades organizacionais** para Data Vaults (consulte "Configurando pela primeira vez" (página 24)).

Para configurar o acesso ao Active Directory:

a. Clique em **Configuração** no painel de navegação esquerdo.

b. Clique em **Configurar Acesso ao Active Directory**.

c. Siga as instruções na janela.

2. **Configurar a diretiva de Cleanup**.

Os Local Repositories do Data Protector for PCs nos computadores dos usuários e os Data Vaults nos Servidores do Data Vault precisam ser limpos periodicamente, para que as versões mais antigas que as configurações de retenção definidas nas diretivas de proteção de arquivos sejam removidas.

Para configurar a diretiva de Cleanup:

a. Clique em **Diretivas** no painel de navegação esquerdo.

b. Clique em **Definir a Diretiva de Cleanup**.

c. Siga as instruções na janela.

Assim esse Data Vault pode dar suporte a mais usuários, executar o processo de cleanup apenas nos fins-de-semana, começando na sexta-feira ou no sábado pela manhã, para que disponha do máximo tempo para ser executado:

a. Abra a página Diretiva de Cleanup no console do administrador do Policy Server e altere o **Agendamento de Cleanup do Data Vault**.

b. Desmarque todos os dias, exceto sexta-feira e sábado:

- Para sexta-feira, escolha uma hora de início no fim da noite, como às 22:00.
- Para sábado, escolha uma hora de início, cedo pela manhã, como à 01:00.

Com o cleanup sendo executado apenas nos fins-de-semana:

- A lista de arquivos apresentada para restauração de um Data Vault estará desatualizada dentro de até uma semana. Os usuários poderão sempre acionar uma nova varredura manual de seus dados no Data Vault para obter uma visualização atualizada.
- As versões em backup ainda existirão além de seu tempo de obsolescência por até uma semana, pois o cleanup é executado apenas nos fins-de-semana.
- O gerenciamento de cotas não está atualizado. Se os usuários excederem sua cota, eles podem precisar esperar até que o cleanup tenha sido executado, para que disponham de espaço livre em seu Data Vault novamente. Por outro lado, exceder a cota pode não ser imediatamente reconhecido pelo sistema, pois o relatório de utilização de espaço faz parte do processo de cleanup.

Prática recomendada:

- **Agendamento de Cleanup do Local Repository**: Mantenha no padrão de 1 hora.
- **Agendamento de Cleanup do Data Vault**: As configurações padrão de "limpar todos os dias à meia-noite" devem ser aceitáveis para a maioria das instalações.

Consulte "Recomendações de dimensionamento" (página 32) para obter mais informações sobre a capacidade do Data Vault.

- Você pode configurar o DPNECleanup para a utilizar vários threads de uma maneira reutilizável e prorrogável, para a melhor utilização da CPU e do disco, permitindo que mais dados sejam armazenados. Consulte "Configurando o cleanup de vários threads" (página 35).

3. **Configurar a diretiva de Controle de Usuário**.

   A diretiva de Controle de Usuário determina quanto controle os usuários terão em relação às diretivas corporativas distribuídas em seus computadores.

   Para configurar a diretiva de Controle de Usuário:

   a. Clique em **Diretivas** no painel de navegação esquerdo.
   b. Clique em **Definir a Diretiva de Controle de Usuário**
   c. Siga as instruções na janela.

   Prática recomendada:

   Defina **permitir controle de usuário** para a **Recuperação de Autoatendimento**.

4. **Configurar a diretiva de Atualização de Agente**.

   A diretiva determina a versão do Agente do Data Protector for PCs que deverá ser usada por todos os desktops e notebooks protegidos pelo Data Protector for PCs, que serão automaticamente atualizados para essa versão.

   Para configurar a diretiva de Atualização de Agente:

   a. Clique em **Diretivas** no painel de navegação esquerdo.
   b. Clique em **Definir a Diretiva de Atualização de Agente**.
   c. Siga as instruções na janela.

5. **Configurar Retenção de Dados para Relatórios**.

   Essa opção define o tempo pelo qual os dados são retidos para fins de relatório para cada uma das principais categorias de informações.

   Para configurar a Retenção de Dados para Relatórios:

   a. Clique em **Configuração** no painel de navegação esquerdo.
   b. Clique em **Configurar Retenção de Dados para Relatórios**.
   c. Siga as instruções na janela.

Outras tarefas de configuração

Geralmente essas tarefas são realizadas assim que o Data Protector for PCs é instalado pela primeira vez.

Licença do software Data Protector for PCs.

Se estiver avaliando o Data Protector for PCs, você pode usá-lo por 60 dias para proteger um número ilimitado de usuários sem a necessidade de outra licença. Quando você

compra o Data Protector for PCs, você precisa acessar o HP License Key Delivery Service em: https://webware.hp.com/welcome.asp, para baixar uma chave de licença, a qual pode ser inserida posteriormente.

Para inserir uma chave de licença:

1. Clique em **Gerenciamento de Licença** no painel de navegação esquerdo.
2. Clique em **Insira uma chave de licença para os usuários do HP Data Protector for PCs**.
3. Siga as instruções na janela.

Se você tiver várias licenças para inserir, pode criar um arquivo de texto com uma string de chave de licença em cada linha. Você pode importar o arquivo usando o campo Importar Chave(s) de Licenças

NOTA As licenças são distribuídas aos Agentes quando os Agentes são instalados.

Movendo Licenças

Se precisar alterar o endereço IP do Policy Server para mover o servidor para outro sistema, ou precisar mover as licenças de um Policy Server para outro, entre em contato com a HP License Key Delivery Service, em: https://webware.hp.com/welcome.asp.

Definir, Importar e Exportar uma senha de criptografia.

Por motivos de segurança, você deve definir uma senha de criptografia antes que possa usar o Data Protector for PCs. Isso garante que todos os arquivos estão criptografados no computador do usuário e são transmitidos criptografados pela rede. A mesma senha é usada para criptografar os arquivos de todos os usuários e para todos os Data Vaults configurados centralmente.

- Um Data Vault definido centralmente (definido através do Console do Policy Server) sempre utilizará a criptografia baseada na senha de criptografia do Data Protector for PCs.
- Com os Data Vaults definidos localmente (definidos pelos usuários através de seus computadores), cada usuário pode escolher se utilizará a criptografia ou não, e escolher suas próprias senhas.

Quando você instala pela primeira vez o Data Protector for PCs, você deve gerar ou importar uma senha antes que possa continuar. Após gerar a senha, para sua segurança, exporte a senha. Assim, ela é salva em um local seguro. Você poderá utilizá-la mais parte para importação.

NOTA Após gerar ou importar uma senha, ela não pode ser alterada.

Para gerenciar sua senha de criptografia:

1. Clique em **Diretivas** no painel de navegação esquerdo.
2. Clique em **Diretiva de Criptografia**.
3. Siga as instruções na janela.

Como determinar quantos Agents podem ser suportados

É difícil apresentar regras gerais que funcionarão em todos os ambientes, assim, os casos apresentados aqui descrevem claramente o contexto para os quais os números dados são válidos.

Fatores que afetam o dimensionamento

Dimensionar um ambiente do Data Protector for PCs é um processo complexo. Os fatores técnicos que influenciam o número de usuários que um ambiente específico pode suportar incluem:

- O poder de processamento no Data Vault (para a consolidação noturna dos dados em backup)
- A rede e a largura da banda de E/S no servidor do Data Vault
- O espaço em disco no servidor do Data Vault
- O tamanho do banco de dados SQL no Policy Server
- A largura de banda da rede e o poder de processamento no Policy Server

Os itens que podem gerar um gargalo em uma determinada instalação são definidos tanto pelas definições de configuração do Data Protector for PCs quanto pelos padrões de utilização:

- O número de usuários em um Data Vault
- O número e o tamanho dos arquivos cobertos pelas diretivas de proteção configuradas
- A frequência de alteração dos arquivos protegidos
- As configurações de retenção para os tipos de arquivos protegidos

Recomendações de dimensionamento

Data Vault

Com um agendamento de cleanup diário, esse Data Vault, com 14 TB de espaço em disco, pode suportar uma população de usuários de até **3.500** Agents, se as características da média de dados forem aproximadamente as seguintes:

- Número médio de arquivos protegidos: 5000
- Tamanho total médio dos arquivos protegidos no disco local: 10 GB
- Tamanho total médio no Data Vault (compactado): 4 GB

Se você precisar proteger uma média de dados maior que a deste exemplo, simplesmente aumentar a capacidade do disco no Data Vault dará mais espaço aos dados, mas o

Data Vault talvez não mais possa concluir a consolidação noturna dos dados em backup em tempo hábil. Considere as seguintes possibilidades:

- Executar o cleanup do Data Vault apenas nos fins-de-semana. Consulte o passo 2 "Configurar a diretiva de Cleanup" em: “Configuração das diretivas restantes” (página 28) para obter detalhes sobre essa ação. Assim, o número de Agentes suportados por um Data Vault com 40 TB de espaço em disco, deve ser aumentado para 10.000, com as mesmas características da média de dados.
- Considere distribuir os dados dos usuários finais entre vários Data Vaults.

As especificações de hardware para esses Data Vaults são as seguintes:

Tipo de Data Vault	Cleanup diária (até 3.500 Agentes)	Cleanup semanal (até 10.000 Agentes)
Compartilhamento de Arquivos do Windows	Dual core de 3 GHz, 4 GB de RAM e 14 TB de espaço em disco	Dual core de 3 GHz, 4 GB de RAM e 40 TB de espaço em disco
Data Vault Web	Quad core de 3 GHz, 4 GB de RAM e 14 TB de espaço em disco	Quad core de 3 GHz, 4 GB de RAM e 40 TB de espaço em disco

Se os seus usuários tiverem menos dados em média, você talvez possa hospedar números de usuários em um Data Vault maiores que esses.

NOTA A HP recomenda veementemente que você mantenha o sistema operacional do Data Vault e os dados em backup em discos separados fisicamente para obter um melhor desempenho.

Para obter um melhor desempenho, o disco do Data Vault deve ser regularmente desfragmentado.

Policy Server

A quantidade de tráfego gerada no Policy Serve depende diretamente do número de Agents hospedados pelo servidor. Usar a edição Express do MS SQL Server, inclusa no Data Protector for PCs, impõe um tamanho de banco de dados máximo de 4 GB, e um limite máximo de 5.000 Agentes.[1] pode ser suportado.

Se você precisar oferecer suporte a mais de 5.000 Agents em seu ambiente, você pode criar Policy Servers adicionais ou substituir o MS SQL Express por uma versão completa do Microsoft SQL Server. Dessa maneira, o Policy Server pode ser facilmente redimensionado para 50.000 Agents. Se você decidir usar a versão completa do MS SQL Server, considere atualizar a memória principal do Policy Server para pelo menos 3 GB.

Por motivos de desempenho, o Policy Server deve ser executado em um servidor separado do Servidor do Data Vault. É possível executá-los no mesmo servidor, mas isso só é recomendado para fins de avaliação.

1. Usar a configuração padrão para a "retenção de dados para relatórios" no Policy Server de 30 dias.

Deve haver pelo menos um Policy Server, mas não é necessário um número igual de Data Vaults e Policy Servers.

Considerações sobre a rede

NOTA Os Data Vaults Web não são afetados pelo alto nível de latência. Estas especificações aplicam-se apenas aos Data Vaults do compartilhamento de arquivos do Windows.

De forma geral, nos Data Vaults do compartilhamento de arquivos do Windows, a HP não recomenda a execução da atualização inicial nos Agents do Data Protector for PCs para os Data Vaults se a latência da rede entre os dois for maior que 50 milésimos de segundo. Isso geralmente se aplica a escritórios domésticos ou remotos em uma conexão WAN lenta. A atualização inicial funcionará, mas levará um tempo muito longo.

Se o seu ambiente incluir escritórios em vários locais, e latência da rede para alguns deles for maior que 50 milésimos de segundo, considere instalar Data Vaults em mais de um local, para que todos os escritórios possam alcançar pelo menos um Data Vault com uma latência de 50 milésimos de segundo ou menos.

Após a atualização inicial ser concluída, as atualizações podem ser realizadas de qualquer local em sua rede corporativa ou até mesmo de um escritório doméstico. Geralmente elas são pequenas o suficiente, de maneira que funcionam bem mesmo em conexões de redes lentas.

Se a atualização inicial precisar ser realizada através de uma conexão de alta latência, ela pode levar vários dias para ser concluída, mas pode ser interrompida sem problemas. O Data Protector for PCs continuará a atualizar até o ponto no qual foi interrompido, assim que se reconectar ao Data Vault.

DICA Se você não souber qual é a latência entre os seus escritórios, use o comando `ping` em um computador em um local para obter o ping de um computador em outro local. Cada ping bem-sucedido informará a latência.

5 Configurando o cleanup de vários threads

O desempenho do `DPNECleanup` limita a quantidade de backup dos dados do usuário em um Data Vault. Você pode configurá-lo de maneira a utilizar vários threads de uma maneira reutilizável e prorrogável, para a melhor utilização da CPU e do disco, permitindo que mais dados sejam armazenados.

Com o Cleanup de vários threads, o argumento Agendador `"-s"` leva aos argumentos padrão `"-e -f -u -p -d 1000"`, incluindo o cleanup de vários threads por padrão, e um atraso de 1 segundo para o Ajustador Automático. Se você não quiser usar esses padrões, por exemplo, para desabilitar a execução de vários threads ou para ajustá-la, exclua o argumento "-s" da chamada do Agendador e anexe argumentos CLI individuais.

NOTA

Embora você possa desejar desabilitar o Cleanup de vários threads em algumas circunstâncias, é recomendado manter `"-e -f -u"` como argumentos para a chamada do Cleanup no Data Vault.

Utilizando o DPNECleanup.exe do CLI

O argumento `-p` para `DPNECleanup.exe` permite que o Cleanup inicialize e inicie o Mecanismo Paralelo e assim habilite a execução de vários threads. O Mecanismo Paralelo oferece sete argumentos de linha de comando opcionais. O executável do DPNECleanup é capaz de recuperar esses argumentos e repassá-los para o Mecanismo Paralelo.

O DPNECleanup será executado no modo serial se `-p` não for definido. Nesse modo, o Mecanismo Paralelo não é usado.

dpnecleanup

`–a` *`afinidade`*

Define a afinidade do processador com um número determinado, o que reflete os bits definidos para os núcleos da CPU que serão usados pelos threads.

`–d` *`atraso`*

Define o atraso em milésimos de segundo até que o Ajustador Automático inicie a funcionar, dando ao Mecanismo Paralelo tempo para iniciar um número de threads e criar uma utilização do sistema. Por padrão, o argumento `–s` leva a um atraso de 1000 milésimos de segundo, ou 1 segundo.

`–m` *`maxCpuUsage`*

Define o máximo de utilização da CPU desejado (em todos os núcleos definidos por `afinidade`) para *`maxCpuUsage`*%, que o Ajustador Automático tentará alcançar. *`maxCpuUsage`* deve ser um número inteiro entre 1 e 100. O padrão é '0', que significa que não há limite (utilização máxima da CPU).

`-o`
Recursos constantes, significando que o Ajustador Automático está desabilitado e o Mecanismo Paralelo não alterará o número de threads simultâneos. Use `-r` para ajustar o número de threads simultâneos. Os argumentos `-d`, `-m` e `-q` são ignorados durante a execução com `o`.

`-p`
Permite o Cleanup de vários threads.

`-q maxQueueLength`
Define a extensão de fila de disco média máxima desejada, a qual o Ajustador Automático tentará alcançar. O valor deve ser um número flutuante. O padrão é 2.0.

`-r resourceCount`
Define o número de recursos (threads) simultâneos a um número determinado. Por padrão e, em combinação com a opção `-o`, o sistema funcionará com 2^(contagem de CPU) threads simultâneos. Se o Ajustador Automático estiver sendo executado, o valor determinado representará o limite de recursos simultâneos em termos de threads. Aqui, o padrão para o número máximo é '0', o que significa que não há limite.

`-z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`
Define a prioridade do processo para todos os threads. O padrão é `Normal`.

`-s`
Cleanup do servidor. Define o Cleanup para todos os Data Vault, sejam eles definidos centralmente ou pelo usuário. Com o comportamento de vários threads, ele é substituído pelos argumentos '`-e -f -u -p -d 1000`' quando o comando é executado.

`-e`
Cleanup corporativa. Define a limpeza para todos os Data Vault definidos centralmente pelas diretivas do Policy Server.

`-f`
Cleanup rápido. Normalmente, o Cleanup do Agente será executado apenas se o sistema estiver no estado ocioso. Essa opção permite que o Cleanup seja iniciado a qualquer hora.

`-u`
Cleanup definido pelo usuário. Define o Cleanup para todos os Data Vaults locais definidos por diretivas locais criadas pelo usuário.

6 Instalando os Agentes do Data Protector for PCs

NOTA As licenças são distribuídas aos Agentes quando os Agentes são instalados.

Os Agentes do Data Protector for PCs podem ser instalados de duas maneiras:

- Individualmente em cada máquina cliente. Consulte "Instalando os Agentes do Data Protector for PCs em máquinas cliente individuais" (página 37).
- Implantados em uma Empresa a partir de um servidor de arquivos acessível a todas as máquinas clientes. Consulte "Implantando os Agents do Data Protector for PCs em uma Empresa" (página 38).

Instalando os Agentes do Data Protector for PCs em máquinas cliente individuais

Pré-requisitos

O software dos Agentes do Data Protector for PCs pode ser instalado nos desktops e notebooks dos usuários que possuem Windows. Para conhecer as plataformas compatíveis, consulte a Matriz de Suporte.

Você deve estar conectado em uma conta com privilégios de "administrador".

Procedimento de instalação

1. Insira o CD-ROM de instalação do Data Protector for PCs. Um assistente de instalação deve ser inicializado automaticamente. Caso ele não seja inicializado, execute-o manualmente clicando duas vezes em `setup.hta` na raiz do CD-ROM de instalação.
2. Clique em **Instalar ou Atualizar o Software do Agente do Data Protector for PCs**. Escolha **Abrir** (ou **Executar**) se uma caixa de diálogo "Abrir ou Salvar" for exibida.
3. Se o computador do usuário não dispor do Microsoft Windows Installer 3.1 ou superior instalado, o assistente poderá instalá-lo. Quando a caixa de diálogo Atualizar Windows Installer for exibida, clique em **OK** para instalá-lo.
4. Se o computador do usuário não dispor do Microsoft .NET Framework 2.0 SP1 ou superior instalado, o assistente poderá instalá-lo. Quando a caixa de diálogo Instalar Microsoft .NET Framework 2.0 SP1 for exibida, clique em **OK** para instalá-lo.
5. O assistente instala automaticamente o Agente do Data Protector for PCs. Siga as instruções na tela. Durante a instalação, você será solicitado a inserir detalhes do Policy Server.

6. Quando a instalação e a configuração estiverem completas, clique em **Concluir**. Se houver uma diretiva de Open File Protection definida no Policy Server, você será solicitado a reinicializar o seu sistema.

   Agora você deve ver o ícone do Data Protector for PCs na bandeja do sistema (um destes, dependendo do status de sua proteção: ).

7. Teste se o Agente do Data Protector for PCs está funcionando adequadamente:
   a. Selecione ou crie um arquivo de teste, como um documento do Word ou uma planilha do Excel, digamos, na Área de Trabalho. Faça algumas alterações a ele e clique em **Salvar**.
   b. Clique com o botão direito no arquivo de teste na Área de Trabalho, no Windows Explorer ou em uma caixa de diálogo Aberta. Três instâncias do Data Protector for PCs deverão aparecer no menu exibido(**Procurar e recuperar arquivos...**, **Copiar Versão** e **Abrir Versão com *XXX...***).
   c. Selecione **Abrir Versão com *XXX...*** e uma lista das versões com indicação de tempo do documento recém-criado e editado. Se você selecionou uma das versões, ela será aberta como um documento somente leitura no aplicativo adequado. É dessa maneira que um usuário recupera uma versão anterior de seus documentos do repositório local do Data Protector for PCs.
8. Repita os passos de 1 a 8 para os desktops e notebooks dos outros usuários que serão protegidos pelo Data Protector for PCs.

Implantando os Agents do Data Protector for PCs em uma Empresa

Você pode implantar inicialmente os Agents do Data Protector for PCs em uma Empresa usando o Kit de Implantação de Agent do Data Protector for PCs contido no CD-ROM de instalação.

NOTA Você não pode usar o Kit de Implantação em PCs com Windows Vista que possuem UAC (Controle de contas de usuários) habilitado. Para corrigir esse problema, desabilite o UAC ou instale o Agente interativamente.

No procedimento descrito abaixo, primeiro você copia o Kit de Implantação do Agent do Data Protector for PCs no *CD-ROM*`:\Agente` para um diretório em um servidor de arquivos acessível a todos os seus usuários. A seguir, você cria um arquivo de parâmetro dentro desse diretório usando `SetupConfig.exe`. Por fim, você estabelece um mecanismo para executar `StartInstall.exe` no diretório compartilhado do computador de cada usuário. Por exemplo, você pode usar um script de logon. Você poderá então monitorar a sua implantação usando o relatório da Implantação do Agent no Console do Policy Server do Data Protector for PCs.

Conteúdo do kit

O Kit de Implantação do Data Protector for PCs contém os seguintes componentes:

`SetupConfig.exe` Cria e edita o arquivo de inicialização.

`StartInstall.exe`	Inicia o `Setup.exe` como um usuário privilegiado.
`Setup.exe`	Instala os pré-requisitos e o `DataProtectorNE.ini`.
`DataProtectorNE.msi`	O pacote do Windows Installer do Data Protector for PCs para instalar o software do Agente.
`DataProtectorNE64.msi`	Pacote do Windows Installer do Data Protector for PCs para instalar o software do Agente em máquinas de 64 bits.
`DataProtectorNE*.*.mst`	O pacote do Windows Installer do Data Protector for PCs para instalar o software do Agente localizado.
`WindowsInstaller.exe`	Atualiza o Windows Installer (obrigatório para a instalação do .NET).
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	Instala o .NET Framework 2.0 SP1
`Setup.ini`	O arquivo do parâmetro de configuração da instalação do Data Protector for PCs. O arquivo será criado com a utilização de `SetupConfig.exe` (consulte o passo 4 abaixo).

Procedimento de implantação e instalação

1. Copie os arquivos no diretório do Agente do CD-ROM de distribuição para um diretório acessível a todos os usuários que pretendem usar o Kit de Implantação do Agent do Data Protector for PCs. Ele pode ser o diretório de um compartilhamento de logon de rede comum, como: `\\yourserver\DPNEDeploy`.
2. Certifique-se de que o diretório recém-criado contenha os arquivos listados acima. Todos os outros arquivos podem ser excluídos.
3. Abra a janela de comando do DOS (`cmd.exe`) e aplique o comando `cd` para o diretório criado no passo 1.
4. Execute `SetupConfig.exe` para criar ou editar o arquivo do parâmetro `Setup.ini`. A primeira vez que `SetupConfig.exe` for executado, é necessário inserir os valores para todos os parâmetros. Após a inserção, você pode executar `SetupConfig.exe` repetidamente para alterar os parâmetros. Se você não desejar alterar um parâmetros, basta pressionar **Enter**.

   Os parâmetros obrigatórios são:

   - **O caminho UNC para os pacotes de instalação** - o caminho completo para o diretório compartilhado no qual os arquivos foram copiados no passo 1, como: `\\yourserver\DPNEDeploy`.
   - O nome do **Policy Server do Data Protector for PCs**. Ele pode ser um nome de NetBIOS, como: `SEUSERVIDOR`, ou um nome de domínio completamente qualificado, como: `seuservidor.suaempresa.com`.
   - **Nome de usuário** - o nome de um usuário com privilégios de Administrador nos computadores que utilizam o Kit de Implantação do Agent do Data Protector

for PCs, como um membro do grupo Administradores do Domínio. Ele geralmente é um nome de usuário completamente qualificado, como `SUAEMPRESA\MarcosAdmin`.

- **Senha** - a senha associada ao Nome de usuário. Você deve digitá-la duas vezes para confirmá-la.

5. No computador cliente, execute `StartInstall.exe`, por exemplo,`\\seuservidor\DPNEDeploy\StartInstall`. Assim, `Setup.exe` será executado em segundo plano, com menor prioridade, utilizando o nome de usuário e a senha especificada em `Setup.ini`. Isso pode ser feito como parte de um script de logon. Observe que você não pode inclui-lo em um script de inicialização, pois a conta da máquina não possui privilégios suficientes na rede.
6. `Setup.exe` define se o computador cliente suporta o Data Protector for PCs. Para conhecer as plataformas Windows compatíveis, consulte a Matriz de Suporte.
7. `Setup.exe` determina se a versão 2.0 SP1 do .NET Framework está instalada. Caso não esteja, ela será instalada, a seguir, pode ser necessário reinicializar o computador.
8. `Setup.exe` define se o Data Protector for PCs já está instalado. Se não estiver ou se a versão estiver desatualizada, ele instala o Data Protector for PCs.

NOTA

Quaisquer erros encontrados nos passos de 4 a 7 acionarão uma mensagem no Policy Server do Data Protector for PCs e no Log de Eventos do Aplicativo no computador local.

Você pode verificar o andamento da implantação do seu Agent usando o Console do Policy Server do Data Protector for PCs:

1. Conecte-se no Console do Policy Server do Data Protector for PCs.
2. Selecione **Implantação do Agentt** em **Relatórios** no painel de navegação esquerdo.

   Você verá um resumo de sua implantação inicial até a data em questão. Ele mostra:

   - Quantas máquinas tiveram sua implantação **concluída** com êxito.
   - O número para o qual a implantação está **em andamento**.
   - O número em que a implantação **falhou**.
3. Clique em um número na coluna **Número de Máquinas** para visualizar uma lista das máquinas no estado de implantação selecionado.

   O status atual de cada máquina é exibido. Por exemplo, se a implantação tiver falhado em uma determinada máquina, a coluna **Informações** apresentará o erro ocorrido. Você pode receber detalhes adicionais sobre uma máquina clicando no nome do NETBIOS.

7 Atualizando o Data Protector for PCs

Se você estiver atualizando uma versão 6.*x* do Data Protector for PCs para a 7.0, siga esta ordem:

1. Atualize o Policy Server para a versão 7.0. Consulte "Atualizando o Policy Server" (página 41).
2. Instale o Servidor do Data Vault Web. Consulte a instalação de um "Instalação, configuração e manutenção do Servidor do Data Vault Web" (página 18) da Web.
3. Atualize os Agentes para a versão 7.0.

   Você pode atualizá-los usando a Atualização Manual ou "silenciosamente" utilizando a Diretiva de Atualização de Agente. Consulte "Atualizando os Agentes" (página 41), para obter mais detalhes.

Atualizando o Policy Server

Você pode atualizar uma instalação existente do Policy Server do Data Protector for PCs para uma versão mais nova, seguindo o procedimento de instalação padrão. Todas as configurações existentes (como a configuração do Data Vault, o Licenciamento etc.) estarão disponíveis na versão mais nova.

Atualizando o Policy Server:

1. Insira o CD-ROM de instalação do Data Protector for PCs. Se o assistente de instalação não for iniciado automaticamente, execute-o manualmente clicando duas vezes em `setup.hta` na raiz do CD-ROM de instalação.
2. Clique em **Instalar Policy Server** na página Instalar o Data Protector for PCs do Data Protector do assistente para iniciar a atualização.
3. Siga as instruções na tela.
4. O procedimento de instalação detectará uma instalação existente do Policy Server e oferecerá uma atualização.
5. Siga as instruções na tela.
6. Quando a instalação for concluída, clique em **Avançar** . Você pode escolher executar o Console do Policy Server do Data Protector for PCs.

NOTA Se o software de Cleanup estiver instalado no Policy Server, também é necessário atualizá-lo. Você pode atualizá-lo manualmente ou utilizando a Diretiva de Atualização de Agente.

Atualizando os Agentes

Se você atualizar a versão do Servidor do Data Protector for PCs, os Agentes existentes que utilizam a versão anterior do Data Protector for PCs continuarão a funcionar como anteriormente. Você pode atualizá-los usando a Atualização Manual ou "silenciosamente" utilizando a Diretiva de Atualização de Agente.

NOTA Após a atualização, todos os Agentes devem ser reinicializados, para que possam utilizar os novos Data Vaults Web. Eles são orientados a isso por balões de mensagens na bandeja do sistema, e também na guia Resumo do Painel da Situação do Data Protector for PCs em seus PCs.

Atualização de Agente automática usando a Diretiva de Atualização de Agente

Os Agentes podem ser atualizados "silenciosamente" com a utilização da Diretiva de Atualização de Agente do Policy Server. O pacote de instalação será distribuído automaticamente a todos os clientes conectados e a atualização será concluída de maneira completamente automatizada. O usuário final não será interrompido.

1. No Console do Policy Server, selecione **Diretivas>Diretiva de Atualização de Agente**.
2. Se você acabou de atualizar o seu Policy Server, o procedimento de instalação carregou um novo Pacote de Atualização de Agente. No Console do Policy Server, essa nova versão não está selecionada ainda.

   Selecione a nova versão do Agente para tornar a versão disponível.
3. Ajustando a Limitação, você pode ajustar o número máximo de atualizações permitidas por minuto.
4. Clique em **Salvar Diretiva de Atualização de Agente**.
5. Agora os Agentes serão atualizados automaticamente para a versão mais atual. Os Agentes de Cleanup também serão atualizados automaticamente.

NOTA Você pode verificar o andamento da atualização do Agente usando o relatório: "Implantação do Agente".

Atualização Manual do Agente

Um Agente existente do Data Protector for PCs pode ser atualizado para uma versão mais atual executando-se o procedimento de instalação padrão.

Antes de atualizar o Agente para uma versão mais atual, certifique-se de que a versão do Agente é compatível com a versão do Policy Server do Data Protector for PCs.

1. Insira o CD-ROM de instalação do Data Protector for PCs. Se o assistente de instalação não for iniciado automaticamente, execute-o manualmente clicando duas vezes em `setup.hta`, na raiz do CD-ROM de instalação.
2. Clique em **Instalar Agente** na página Instalar Data Protector for PCs do assistente para iniciar a atualização.
3. Siga as instruções na tela.
4. O procedimento de instalação detectará uma instalação existente do Agente e oferecerá uma atualização.
5. Siga as instruções na tela.

8 Como obter suporte para o Data Protector for PCs

O Data Protector for PCs é distribuído com um ano de manutenção. Isso dá o direito a:

- Suporte por telefone, fale com um Técnico de Suporte.
- atualizações do Servidor do Data Protector for PCs e do software Agent do Data Protector for PCs. Você pode baixar as versões mais atuais ou uma imagem de CD-ROM do site do Data Protector. Acesse: http://www.hp.com/go/dataprotector.

Glossário

Active Directory *(Termo específico do Windows)* O serviço de diretórios em uma rede do Windows. Ele contém informações sobre os recursos na rede, permitindo que eles sejam acessados por usuários e aplicativos. Os serviços de diretórios oferecem uma maneira consistente para nomear, descreve, localizar, acessar e gerenciar os recursos independentemente do sistema físico no qual eles se encontra.

Agent O software do Data Protector for PCs que é executado no desktop/notebook de cada usuário. Ele se comunica com o Policy Server através dos serviços Web (SOAP e XML) pela porta 80 do TCP.

arquivos protegidos Um arquivo protegido é aquele cujo backup é automaticamente feito pelo Data Protector for PCs. Os tipos de arquivos protegidos são definidos nas diretivas de Continuous e Open File Protection.

atualização inicial O Data Protector for PCs protege os arquivos continuamente à medida que os usuários os modificam salvando suas alterações. Sempre que um usuário criar um novo Data Vault, o Data Protector for PCs deve fazer uma atualização inicial dos arquivos protegidos de todos os usuários no vault. Os usuários podem selecionar a maneira como a atualização inicial é feita, imediatamente ou em segundo plano.

console O console baseado em navegador é o local onde as diretivas do Data Protector for PCs são definidas centralmente. Você precisa ser um membro do grupo do Administrador.

Continuous File Protection A Continuous File Protection é o método de Continuous Data Protection do Data Protector for PCs, que armazena automaticamente as alterações feitas em um arquivo, sempre que esse arquivo é salvo. Ela é adequada a arquivos de dados salvos pelo usuário (em contraste com arquivos sempre abertos, como bancos de dados ou arquivos do Outlook). Cada diretiva de Continuous File Protection protege um grupo de arquivos que se relacionam de alguma maneira. O Data Protector for PCs é oferecido pré-configurado com políticas para tipos de arquivos comumente usados, como Documentos e Imagens do Office. Você pode editar essas Diretivas de Proteção de Arquivos ou criar suas próprias. A diretiva também especifica o tempo pelo qual as versões anteriores dos arquivos protegidos são retidos.

Data Vault Há dois tipos de Data Vault:

- Data Vaults Web. Eles usam o protocolo HTTPS e proporcionam o melhor nível de segurança para a transmissão de dados entre PCs clientes e o Data Vault, melhorando a taxa de transferência em ambientes de alta latência, sendo mais recomendados.
- Data Vaults do compartilhamento de arquivos do Windows. São pastas compartilhadas em um servidor de arquivos no qual os arquivos são armazenados de acordo com uma diretiva do Data Vault. O servidor de arquivos deve ser compatível com o protocolo de compartilhamento de arquivos do Windows (CIFS/SMB). Eles não devem ser usados em ambientes com um alto nível de latência de rede.

A estrutura de dados desses dois tipos de Data Vault é a mesma, assim, os Data Vaults do compartilhamento de arquivos do Windows podem ser convertidos em Data Vaults Web.

Podem ser atribuídas aos usuários uma ou mais políticas de Data Vault, de acordo com sua participação em um grupo ou unidade organizacional.

diretiva Uma diretiva é um conjunto de regras, definida centralmente no Policy Server e executada pelo Agent em cada desktop/notebook.

Diretiva de Cleanup Os períodos de retenção definidos pelas diretivas de proteção de arquivos são aplicados pelas tarefas de cleanup executadas periodicamente. A frequência é definida na diretiva de Cleanup. Por padrão, os Local Repositories dos usuários são limpos a cada hora e, qualquer Data Vault

definido localmente é limpo uma vez por dia. Os Data Vaults do compartilhamento de arquivos do Windows definidos centralmente são limpos por um computador atribuído por meio da Diretiva do Data Vault, já os Data Vaults Web pelo cleanup executado localmente no Servidor do Data Vault. A diretiva de cleanup aplica-se a todos os usuários.

Diretiva de Controle de Usuário

A diretiva determina o nível de controle que usuários individuais possuem sobre o software Agentexecutado em seus desktops/notebooks. Você pode bloquear o Agentde maneira que as diretivas fiquem completamente ocultas para os usuários, você pode permitir que eles vejam as diretivas, mas não as alterem, ou você pode permitir que eles adicionem suas próprias diretivas. Você pode definir separadamente o nível de controle sobre cada uma das principais diretivas do Data Protector for PCs. A diretiva de controle de usuário aplica-se a todos os usuários.

Diretiva de cópia

As diretivas de Cópia definem o seguinte:

- Quantos Agent podem copiar arquivos simultaneamente a seus Data Vaults.
- Um agendamento de atualizações periódicas, que verifica se todos os arquivos esperados para um usuários existem no Data Vault e, se não existirem, copia os arquivos ausentes. O que oferece maior garantia de os arquivos de todos os usuários foram adequadamente copiados para o Data Vault.
- Caso uma *atualização inicial* deva ser executada. A atualização inicial é necessário, pois, durante a operação regular doData Protector for PCs, cada vez que um usuário altera um arquivo protegido continuamente do Data Protector for PCs, apenas as informações sobre as alterações são copiadas para o Data Vault.

Se você acabou de instalar o Data Protector for PCs, é necessário definir a diretiva de Cópia para fazer uma atualização inicial dos arquivos protegidos de todos os seus usuários.

Local Repository

O Local Repository é um local de armazenamento seguro nos computadores Agent utilizado para o armazenamento de arquivos protegidos e alterações dos arquivos, geralmente na unidade de disco rígido do sistema. Ele é um diretório oculto do sistema. Os usuários podem recuperar rapidamente uma versão anterior clicando com o botão direito no arquivo na Área de Trabalho, no Windows Explorer ou em uma caixa de diálogo Aberta. Os arquivos protegidos por diretivas de Continuous File Protection são mantidos em um diretório oculto no computador local até que não mais satisfaçam o período de retenção. Os arquivos protegidos pelas diretivas de Open File Protection são armazenados temporariamente no Armazenamento de Versão local, apenas até que sejam copiados para o Data Vault. O caminho do Local Repository geralmente é `C:\{DPNE}`.

Open File Protection

A Open File Protection faz o backup de arquivos que estão sempre abertos, como Pastas Pessoais do Outlook e vários arquivos de bancos de dados, fazendo periodicamente instantâneos do nível dos arquivos. Às vezes, isso é chamado de Continuous Data Protection "aproximada". Uma diretiva de Open File Protection define a proteção para arquivos abertos, definida por conjuntos de regras de inclusão e exclusão. Por exemplo, você pode definir uma política de nome "Pastas Pessoais do Outlook" que se aplica aos arquivos .pst do Outlook especificando uma regra de inclusão como "terminado em '.pst'". Se desejar excluir os arquivos .pst arquivados, você então poderia criar uma regra de exclusão como "contém 'archive'". As diretivas também especificam o tempo pelo qual as versões anteriores dos arquivos protegidos são retidas. As diretivas de Open File Protection aplicam-se a todos os usuários.

Policy Server

O Policy Server fornece gerenciamento central das diretivas do Data Protector for PCs. Ele também coleta as informações de status dos Agents e fornece relatórios sobre sua implantação e operação.

Usuário Administrativo

Um usuário no Servidor do Data Vault Web que supervisiona as tarefas administrativas, como a criação e exclusão de Data Vaults e a migração de dados de backup do cliente.

Usuário de Backup Um usuário no Servidor do Data Vault Web que executa operações de usuário final, como o backup e a restauração de arquivos.

Índice Remissivo

T

U

V

W