Dell Data Protection

Guia de Recuperação para File/Folder Encryption, Hardware Crypto Accelerator, Unidades de criptografia automática e Chave de uso geral

8.10

© 2016 Dell Inc.

Marcas comerciais registradas e marcas comerciais usadas na suítes de documentos Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools e Dell Data Protection | Cloud Edition Suite: Dell™ e o logotipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance® e o logotipo da Cylance são marcas registradas da Cylance, Inc. nos Estados Unidos e em outros países. McAfee® e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, Inc. nos Estados Unidos e em outros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas registradas da Intel Corporation nos Estados Unidos e em outros países. Adobe®, Acrobat® e Flash® são marcas registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registradas da Authen Tec. AMD® é marca comercial registrada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, e Visual C++® são marcas comerciais ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países. VMware® é marca registrada ou marca comercial da VMware, Inc. nos Estados Unidos ou em outros países. Box® é marca registrada da Box. Dropbox℠ é marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas registradas da Google Inc. nos Estados Unidos e em outros países. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® são marcas de serviço, marcas comerciais ou marcas registradas da Apple, Inc. nos Estados Unidos e/ou em outros países. GO ID®, RSA® e SecurID® são marcas registradas da EMC Corporation. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registrada da Entrust®, Inc. nos Estados Unidos e em outros países. InstallShield® é marca registrada da Flexera Software nos Estados Unidos, China, Comunidade Europeia, Hong Kong, Japão, Taiwan e Reino Unido. Micron® e RealSSD® são marcas registradas da Micron Technology, Inc. nos Estados Unidos e em outros países. Mozilla® Firefox® é marca registrada da Mozilla Foundation nos Estados Unidos e/ou em outros países. iOS® é marca comercial ou marca registrada da Cisco Systems, Inc. nos Estados Unidos e em determinados países e é usada nos Estados Unidos sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou de suas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários. SAMSUNG™ é marca comercial da SAMSUNG nos Estados Unidos ou em outros países. Seagate® é marca registrada da Seagate Technology LLC nos Estados Unidos e/ou em outros países. Travelstar® é marca registrada da HGST, Inc. nos Estados Unidos e em outros países. UNIX® é marca registrada da The Open Group. VALIDITY™ é marca comercial da Validity Sensors, Inc. nos Estados Unidos e em outros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas registradas da VeriSign, Inc. ou suas afiliadas ou subsidiárias nos Estados Unidos e em outros países e licenciadas para a Symantec Corporation. KVM on IP® é marca registrada da Video Products. Yahoo!® é marca registrada da Yahoo! Inc.

Este produto usa partes do programa 7-Zip. O código-fonte pode ser encontrado em www.7-zip.org. O licenciamento é feito sob a licença GNU LGPL + restrições unRAR (www.7-zip.org/license.txt).

2016-07

Protegido por uma ou mais patentes dos EUA, incluindo: Número 7665125; Número 7437752; e Número 7665118.

As informações neste documento estão sujeitas a alterações sem aviso.

Índice

1

Introdução

Esta seção detalha o que é necessário para criar o ambiente de recuperação.

- Cópia obtida por download do software do ambiente de recuperação - Localizada na pasta Kit de recuperação do Windows na mídia de instalação do Dell Data Protection.
- Mídia CD-R, DVD-R ou mídia USB formatada
  - Se estiver gravando um CD ou DVD, verifique o Apêndice A - Gravação do ambiente de recuperação para obter detalhes.
  - Se estiver usando mídia USB, verifique o Apêndice A - Gravação do ambiente de recuperação para obter detalhes.
- Pacote de recuperação para dispositivo com falha
  - Para clientes gerenciados remotamente, as instruções a seguir explicam como obter um pacote de recuperação do Servidor do Dell Data Protection.
  - Para clientes gerenciados localmente, o pacote de recuperação foi criado durante a configuração em uma unidade de rede compartilhada ou em uma mídia externa. Encontre este pacote antes de continuar.

2

Recuperação de File/Folder Encryption

Com a recuperação de FFE (File/Folder Encryption - Criptografia de pastas/arquivos), você pode acessar:

- Um computador que não inicializa e que mostra um prompt para executar uma recuperação de SDE.
- Um computador cujos dados criptografados não podem ser acessados ou cujas políticas não podem ser editadas.
- Um servidor com o Dell Data Protection | Server Encryption que atenda uma das condições acima.
- Um computador com uma placa de Hardware Crypto Accelerator ou uma placa-mãe/TPM que precisa ser trocada.

Requisitos de recuperação

Para a recuperação de FFE, você precisa de:

- Kit de recuperação do Windows para criar um disco de inicialização especial - O kit contém arquivos que serão usados para criar uma imagem do Windows PE (WinPE) e personalizá-la com software e drivers do Dell Data Protection. O kit está situado na pasta Kit de recuperação do Windows na mídia de instalação do Dell Data Protection.

Visão geral do processo de recuperação

Para recuperar um sistema que falhou:

1. Crie uma ISO de recuperação e grave-a em um CD/DVD ou crie uma unidade USB inicializável. Consulte Apêndice A - Gravação do ambiente de recuperação.
2. Obtenha o arquivo de recuperação.
3. Execute a recuperação.

Executar recuperação de FFE

Execute este procedimento para realizar uma recuperação de FFE.

Obter o arquivo de recuperação - Computador gerenciado remotamente

Para fazer download do arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe**:

1. Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento > Recuperar endpoint**.
2. No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
3. Na janela Recuperação avançada, digite uma senha de recuperação e clique em **Fazer download**.

NOTA: Você precisa memorizar essa senha para acessar as chaves de recuperação.

4. Copie o arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe** para um local no qual possa ser acessado quando inicializado no WinPE.

Obter o arquivo de recuperação - Computador gerenciado localmente

Para obter o arquivo de recuperação do Personal Edition:

1. Localize o arquivo de recuperação com o nome **LSARecovery_<nomedosistema>.exe**. O arquivo estava armazenado em uma unidade de rede ou um armazenamento removível quando você acessou o Assistente de configuração durante a instalação do Personal Edition.
2. Copie o arquivo **LSARecovery_<nomedosistema>.exe** para o computador de destino (o computador cujos dados serão recuperados).

Executar uma recuperação

1. Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar. Um ambiente WinPE é aberto.
2. Digite **x** e pressione **Enter** para abrir um prompt de comando.
3. Navegue até o arquivo de recuperação e abra-o.
4. Selecione uma opção:
   - Meu sistema não inicializa e mostra uma mensagem solicitando a execução da Recuperação de SDE.

     Isso permitirá que você recompile as verificações de hardware que o cliente Encryption executa quando você inicializa no SO.
   - Meu sistema não me permite acessar dados criptografados, editar políticas ou está sendo reinstalado.

     Use isso se a placa do Hardware Crypto Accelerator ou a placa-mãe/TPM precisar ser substituída.
5. Na caixa de diálogo Informações de backup e recuperação, confirme que as informações sobre o computador cliente a ser recuperado estão corretas e clique em **Avançar**.

   Ao recuperar computadores que não sejam Dell, os campos SerialNumber e AssetTag estarão em branco.
6. Na caixa de diálogo que mostra uma lista dos volumes do computador, selecione todas as unidades aplicáveis e clique em **Avançar**.

   Use as teclas Shift e Control para destacar múltiplas unidades.

   Se a unidade selecionada não estiver criptografa com FFE, ela não poderá ser recuperada.
7. Digite sua senha de recuperação e clique em **Avançar**.

   Com um cliente gerenciado remotamente, esta é a senha fornecida na Etapa 3 em Obter o arquivo de recuperação - Computador gerenciado remotamente.

   No Personal Edition, a senha é a Senha de administrador do Encryption definida para o sistema no momento em que as chaves foram depositadas.
8. Na caixa de diálogo Recuperação, clique em **Recuperar**. O processo de recuperação é iniciado.
9. Quando a recuperação for concluída, clique em **Concluir**.

NOTA: Remova qualquer mídia USB ou CD\DVD usado para inicializar a máquina. Se não fizer isso, o computador pode ser inicializado novamente no ambiente de recuperação.

10. Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

3

Recuperação de Hardware Crypto Accelerator

Com a Recuperação de Hardware Crypto Accelerator (HCA) do Dell Data Protection, você pode recuperar o acesso para o seguinte:

- Arquivos em uma unidade com criptografia de HCA - Este método descriptografa a unidade usando as chaves fornecidas. Durante o processo de recuperação você poderá selecionar a unidade específica que precisa ser descriptografada.
- Uma unidade com criptografia de HCA após uma substituição de hardware - Este método é usado após a substituição de uma placa do Hardware Crypto Accelerator ou de uma placa-mãe/TPM. Você pode executar uma recuperação para obter acesso novamente aos dados criptografados sem descriptografar a unidade.

Requisitos de recuperação

Para uma recuperação de HCA, você precisará de:

- Acesso a uma ISO do ambiente de recuperação
- Mídia USB ou CD\DVD inicializável

Visão geral do processo de recuperação

Para recuperar um sistema que falhou:

1. Crie uma ISO de recuperação e grave-a em um CD/DVD ou crie uma unidade USB inicializável. Consulte Apêndice A - Gravação do ambiente de recuperação.
2. Obtenha o arquivo de recuperação.
3. Execute a recuperação.

Executar recuperação de HCA

Execute este procedimento para realizar uma recuperação de HCA.

Obter o arquivo de recuperação - Computador gerenciado remotamente

Para fazer download do arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe** gerado quando você instalou o Dell Data Protection:

1. Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento > Recuperar endpoint**.
2. No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
3. Na janela Recuperação avançada, digite uma senha de recuperação e clique em **Fazer download**.

NOTA: Você precisa memorizar essa senha para acessar as chaves de recuperação.

O arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe** é obtido por download.

Obter o arquivo de recuperação - Computador gerenciado localmente

Para obter o arquivo de recuperação do Personal Edition:

1. Localize o arquivo de recuperação com o nome **LSARecovery_<nomedosistema>.exe**. O arquivo foi armazenado em uma unidade de rede ou um armazenamento removível quando você enviou pelo Assistente de configuração durante a instalação do Personal Edition.
2. Copie o arquivo **LSARecovery_<nomedosistema>.exe** para o computador de destino (o computador cujos dados serão recuperados).

Executar uma recuperação

1. Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar.

   Um ambiente WinPE é aberto.
2. Digite **x** e pressione **Enter** para abrir um prompt de comando.
3. Navegue até o arquivo de recuperação salvo e abra-o.
4. Selecione uma opção:
   - Desejo descriptografar minha unidade criptografada HCA.
   - Desejo restaurar o acesso à minha unidade criptografada HCA.
5. Na caixa de diálogo Backup e Recuperação, confirme que a Etiqueta de serviço ou o Número do ativo está correto e clique em **Avançar**.
6. Na caixa de diálogo que mostra uma lista dos volumes do computador, selecione todas as unidades aplicáveis e clique em **Avançar**.

   Use as teclas Shift e Control para destacar múltiplas unidades.

   Se a unidade selecionada não estiver criptografa com HCA, ela não poderá ser recuperada.
7. Digite sua senha de recuperação e clique em **Avançar**.

   Em um computador gerenciado remotamente, essa senha é a senha fornecida na Etapa 3 em Obter o arquivo de recuperação - Computador gerenciado remotamente.

   Em um computador gerenciado localmente, essa senha é a Senha de administrador do Encryption definida para o sistema no Personal Edition no momento em que as chaves foram depositadas.
8. Na caixa de diálogo Recuperação, clique em **Recuperar**. O processo de recuperação é iniciado.
9. Quando solicitado, navegue até o arquivo de recuperação salvo e clique em **OK**.

   Se você estiver executando uma descriptografia completa, a caixa de diálogo a seguir mostrará o status. Esse processo pode exigir algum tempo.
10. Após ser mostrada uma mensagem indicando que a recuperação foi concluída satisfatoriamente, clique em **Concluir**. O computador será reinicializado.

Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

4

Recuperação de Unidade de criptografia automática (SED)

Com a recuperação de SED, você pode recuperar o acesso aos arquivos em uma SED (Self-Encrypting Drive - Unidade de criptografia automática) através dos seguintes métodos:

- Execute o desbloqueio de uso único da unidade para ignorar e remover a Autenticação de pré-inicialização (PBA, Preboot Authentication).
  - Com um cliente SED gerenciado remotamente, posteriormente, a PBA poderá ser ativada novamente através do Remote Management Console.
  - Com um cliente SED gerenciado localmente, a PBA poderá ser ativada através do Security Tools Administrator Console.
- Desbloqueie e, em seguida, remova permanentemente a PBA da unidade. O Login único não funcionará com a PBA removida.
  - Com um cliente SED gerenciado remotamente, se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto a partir do Remote Management Console.
  - Com um cliente SED gerenciado localmente, se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto dentro do SO.

Requisitos de recuperação

Para uma recuperação de SED, você precisará de:

- Acesso à ISO do ambiente de recuperação
- Mídia USB ou CD\DVD inicializável

Visão geral do processo de recuperação

Para recuperar um sistema que falhou:

1. Crie uma ISO de recuperação e grave-a em um CD/DVD ou crie uma unidade USB inicializável. Consulte Apêndice A - Gravação do ambiente de recuperação.
2. Obtenha o arquivo de recuperação.
3. Execute a recuperação.

Executar recuperação de SED

Execute este procedimento para realizar uma recuperação de SED.

Obter o arquivo de recuperação - Cliente SED gerenciado remotamente

1 Obtenha o arquivo de recuperação.

O arquivo de recuperação pode ser obtido por download a partir do Remote Management Console. Para fazer download do arquivo *<nomedehost>-sed-recovery.dat* gerado quando você instalou o Dell Data Protection:

- **a** Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento > Recuperar dados** e, em seguida, selecione a guia **SED**.
- **b** Na tela Recuperar dados, no campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
- **c** No campo SED, selecione uma opção.
- **d** Clique em **Criar arquivo de recuperação**.

  O arquivo **<nome de host>-sed-recovery.dat** é obtido por download.

Obter o arquivo de recuperação - Cliente SED gerenciado localmente

1 Obtenha o arquivo de recuperação.

O arquivo foi gerado e pode ser acessado a partir do local de backup que você selecionou quando o Dell Data Protection | Security Tools foi instalado no computador. O nome do arquivo é *OpalSPkey<nomedosistema>.dat*.

Executar uma recuperação

1 Usando a mídia inicializável criada, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar. Um ambiente WinPE é aberto com o aplicativo de recuperação.

2 Escolha a opção um e pressione **Enter**.

3 Selecione **Procurar**, encontre o arquivo de recuperação e, em seguida, clique em **Abrir**.

4 Selecione uma opção e clique em **OK**.

- **Desbloqueio de uso único da unidade** - Este método ignora e remove a PBA. Posteriormente, a PBA poderá ser ativada novamente através do Remote Management Console (para um cliente SED gerenciado remotamente) ou através do Security Tools Administrator Console (para um cliente SED gerenciado localmente).
- **Desbloquear a unidade e remover a PBA** - Este método desbloqueia e, em seguida, remove permanentemente a PBA da unidade. Se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto a partir do Remote Management Console (para um cliente SED gerenciado remotamente) ou de dentro do SO (para um cliente SED gerenciado localmente). O Login único não funcionará com a PBA removida.

5 A recuperação agora está concluída. Pressione qualquer tecla para retornar ao menu.

6 Pressione **r** para reinicializar o computador.

NOTA: Remova qualquer mídia USB ou CD\DVD usado para inicializar o computador. Se não fizer isso, o computador pode ser inicializado novamente no ambiente de recuperação.

7 Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

5

Recuperação de Chave de uso geral

A Chave de uso geral (GPK - General Purpose Key) é usada para criptografar parte do registro de usuários do domínio. Entretanto, durante o processo de inicialização, em casos raros, ela pode se corromper e não desselar. Nesse caso, os seguintes erros serão mostrados no arquivo CMGShield.log no computador cliente:

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Se a GPK não desselar, ela precisará ser recuperada extraindo-a do pacote de recuperação que é obtido por download do servidor.

Recuperar a GPK

Obter o arquivo de recuperação

Para fazer download do arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe** gerado quando você instalou o Dell Data Protection:

1. Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento > Recuperar endpoint**.
2. No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.

3 Na janela Recuperação avançada, digite uma senha de recuperação e clique em **Fazer download**

NOTA: Você precisa memorizar essa senha para acessar as chaves de recuperação.

O arquivo **LSARecovery_<nomedamáquina_domínio.com>.exe** é obtido por download.

Executar uma recuperação

1 Usando a mídia inicializável criada no Apêndice A - Gravação do ambiente de recuperação, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar.

Um ambiente WinPE é aberto.

2 Digite **x** e pressione **Enter** para abrir um prompt de comando.

3 Navegue até o arquivo de recuperação e abra-o.

Uma caixa de diálogo Diagnóstico do cliente Encryption é aberta e o arquivo de recuperação é gerado em segundo plano.

4 Em um prompt de comando administrativo, execute **LSARecovery_<nomedamáquina_domínio.com>.exe –p <senha> -gpk**

Ele retorna o arquivo GPKRCVR.txt para o seu computador.

5 Copie o arquivo **GPKRCVR.txt** para a raiz da unidade do computador em que está o SO.

6 Reinicie o computador.

O arquivo GPKRCVR.txt será usado pelo sistema operacional para restaurar a GPK nesse computador.

7 Se for solicitado, reinicie novamente o computador.

6

Recuperação de dados de unidade criptografada

Se o computador de destino não for reinicializável e não houver nenhuma falha de hardware, a recuperação de dados pode ser realizada no computador inicializado em um ambiente de recuperação. Se não for possível inicializar o computador de destino e houver falha de hardware ou for um dispositivo USB, a recuperação de dados pode ser realizada inicializando em uma unidade escrava. Quando você define uma unidade como escrava, você pode ver o sistema de arquivos e navegar pelos diretórios. Contudo, se você tentar abrir ou copiar um arquivo, um erro de *Acesso negado* ocorrerá.

Recuperar dados de unidade criptografada

Para recuperar dados de uma unidade criptografada:

1. Para obter o DCID/ID de recuperação do computador, escolha uma das opções:
   a. Executar o WSScan em uma pasta que tem dados criptografados Comuns armazenados.
      O DCID/ID de recuperação de oito dígitos é exibido após “Comum”.
   b. Abra o Remote Management Console, e selecione a guia **Detalhes e ações** para o endpoint.
   c. Na seção Detalhes do Shield da tela Detalhe do endpoint, encontre o DCID/ID de recuperação.

2 Para fazer download da chave do servidor, procure e execute o utilitário Dell Administrative Unlock (**CMGAu**).

O utilitário Dell Administrative Unlock pode ser obtido do Dell ProSupport.

3 Na caixa de diálogo Dell Administrative Utility (CMGAu), digite as informações a seguir (alguns campos podem já estar preenchidos) e clique em **Avançar**.

Servidor:	Nome de host totalmente qualificado do servidor, por exemplo:
	Device Server: **https://<servidor.organização.com>:8081/xapi**
	Security Server: **https://<servidor.organização.com>:8443/xapi/**
Admin Dell:	O nome da conta do Administrador forense (ativado no servidor)
Senha de admin Dell:	A senha da conta do Administrador forense (ativado no servidor)
MCID:	Apague o campo MCID
DCID:	O DCID/ID de recuperação que você obteve anteriormente.

4 Na caixa de diálogo Dell Administrative Utility, selecione **Não, executar um download de um servidor agora** e clique em **Avançar**.

NOTA: Se o cliente Encryption não estiver instalado, uma mensagem é exibida informando que ocorreu uma *Falha no desbloqueio*. Mova para um computador com o cliente Encryption instalado.

5 Quando terminar o download e o desbloqueio, copie os arquivos que você precisa recuperar desta unidade. Todos os arquivos podem ser lidos. ***Não clique em Concluir até ter recuperado os arquivos***.

6 Após recuperar os arquivos e estar pronto para bloquear os arquivos novamente, clique em **Concluir**.

Após clicar em Concluir, os arquivos criptografados não estarão mais disponíveis.

7

Recuperação do BitLocker Manager

Para recuperar dados, você obtém uma senha de recuperação ou um pacote de chaves do Remote Management Console que permitem o desbloqueio dos dados no computador.

Recuperar dados

1. Como um administrador Dell, faça login no Remote Management Console.
2. No painel esquerdo, clique em **Gerenciamento > Recuperar dados**.
3. Clique na guia *Gerenciador*.
4. Para *BitLocker*:

   Digite o **ID de recuperação** recebido do BitLocker. Opcionalmente, se você inserir o Nome de host e o Volume, o ID de recuperação é preenchido.

   Clique em **Obter senha de recuperação** ou em **Criar pacote de chaves**.

   Dependendo de como deseja fazer a recuperação, você usará essa senha de recuperação ou o pacote de chaves para recuperar dados.

   Para o *TPM*:

   Digite o **Nome de host**.

   Clique em **Obter senha de recuperação** ou em **Criar pacote de chaves**.

   Dependendo de como deseja fazer a recuperação, você usará essa senha de recuperação ou o pacote de chaves para recuperar dados.
5. Para concluir a recuperação, consulte as Instruções de recuperação da Microsoft.

NOTA: Se o BitLocker Manager não for "proprietário" do TPM, a senha do TPM e o pacote de chaves não estarão disponíveis no banco de dados Dell. Você receberá uma mensagem de erro informando que a Dell não consegue localizar a chave, que é o comportamento esperado.

Para recuperar um TPM que é "propriedade" de uma entidade que não seja o BitLocker Manager, você deverá seguir o processo para recuperar o TPM desse proprietário específico ou seguir o seu próprio processo existente de recuperação do TPM.

A

Apêndice A - Gravação do ambiente de recuperação

Gravação da ISO do ambiente de recuperação em um CD\DVD

O link a seguir contém o processo necessário para usar o Microsoft Windows 7/8/10 para criar um CD ou DVD inicializável para o ambiente de recuperação.

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

Gravação do ambiente de recuperação em mídia removível

Para criar uma unidade USB inicializável, siga as instruções deste artigo da Microsoft:

https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx


0XXXXXA0X